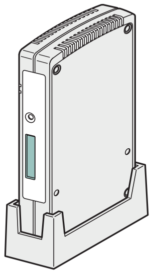
RICOH

Remote Communication Gate A

使用説明書



ご使用の前に、本書を最後までよくお読みの上、正しくお使いください。安全に正しくお使いいただくために、操作の前には必ず『安全上のご注意』をお読みください。

はじめに

このたびは本製品をご利用いただき、ありがとうございます。

株式会社 リコー

東京都中央区銀座 8-13-1 リコービル 〒 104-8222

この本の読みかた

正しくお使いいただくために

このたびは本製品をご利用いただき、ありがとうございます。

この使用説明書は、製品の正しい使い方や使用上の注意について記載してあります。ご使用の前に、この使用説明書を最後までよくお読みの上、正しくお使いください。また、この使用説明書が必要になったとき、すぐに利用できるように保管してください。

マークについて

本書で使われているマークには次のような意味があります。

重要

誤って操作をすると、データ消失などの原因になることがあります。必ず、お読みください。

補足

操作するときに気を付けることや、操作を誤ったときの対処方法などを説明しています。

参照

参照先を示します。

[ ]

画面のキーや項目の名称を示します。

本書についてのご注意

本書の内容に関しては、将来予告なしに変更することがあります。

機械の改良変更等により、本書のイラストや記載事項とお客様の機械とが一部異なる場合がありますのでご了承ください。

画面の表示内容やイラストは機種、オプションによって異なります。

本書は、原則的にオプションを装着した状態の画面と外観イラストを使って説明しています。

略称について

本書では、「Remote Communication Gate A」を「RC Gate」と略して記載しています。指定のない場合、管理者とは RC Gate 管理者を指します。

画面について

本書では、Microsoft® Windows® XP および Internet Explorer 6.0 の画面を用いて説明しています。一部、Microsoft® Windows® 7 および Internet Explorer 9.0 の画面を用いています。ほかの OS をご使用の場合、画面が異なりますが、操作は同じです。

使用説明書の紹介

お使いになる目的に応じて、必要な使用説明書をお読みください。

使用説明書（本書）

本機の使用方法に関するすべての項目が記載されています。『安全上のご注意/セットアップガイド』に記載されている手順を行ったあと、本書の手順を行ってください。

安全上のご注意/セットアップガイド

本機の設置・設定方法と注意事項が記載されています。

補足

- カスタマーエンジニアが本機の設置・登録作業を行った場合は、本書に記載されている登録作業を行う必要はありません。ただし、保守・運用作業を行う場合には本書をよくお読みください。
- PDF 形式の使用説明書を表示するためには、Adobe Acrobat または Adobe Reader が必要です。

おことわり

- 大切な文書やデータは必ずコピーしてください。お客様が操作をミスしたり本製品に異常が生じた場合、文書やデータが消失することがあります。また、コンピューターウイルス、ワーム、そのほかの有害なソフトウェア等に対しては、お客様の責任で必ず予防措置を講じてください。
- お客様が本製品を使用して作成した文書やデータに関し、当社は一切その責任を負えませんのであらかじめご了承ください。
- 本製品の故障による損害、文書やデータの消失による損害、そのほか本製品の使用により生じた損害について、当社は一切その責任を負えませんのであらかじめご了承ください。
- 本製品および使用説明書を運用した結果の影響については、いっさい責任を負いかねますのでご了承ください。

商標

- Adobe、Acrobat、Acrobat Reader、Adobe Reader、Flash は Adobe Systems Incorporated（アドビ システムズ社）の米国ならびにその他の国における登録商標または商標です。
- Microsoft®、Windows®、Internet Explorer®は、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。
- その他の会社名、製品名は、各社の商標または登録商標です。本書の説明および所有者の権利のために使用されます。この使用によって所有者の権利を侵害するものではありません。

  この製品には、OpenSSL Toolkit で使用するために OpenSSL Project によって開発されたソフトウェアが含まれています。(http://www.openssl.org/)
- Windows XP の製品名は以下のとおりです。

  Microsoft® Windows® XP Professional

  Microsoft® Windows® XP Home Edition

目次

3. オートディスカバリー設定ウィザードの操作手順

4. 登録内容の詳細を参照・変更する

5. 付録

1. RC Gate について

ここでは、RC Gate の概要について説明します。

RC Gate を使ってできること

RC Gate を使って、以下の操作ができます。

- デバイスが故障した場合に、RS センターシステムへのサービスコールを自動で発信できます。
- デバイスのファームウェアを更新できます。
- デバイスのカウンター情報を取得し、RS センターシステムに通知できます。
- トナーなど、デバイスの消耗品の残量が少なくなった場合に、自動で発注できます。
- 複数のデバイスの利用状況を簡単に把握できます。

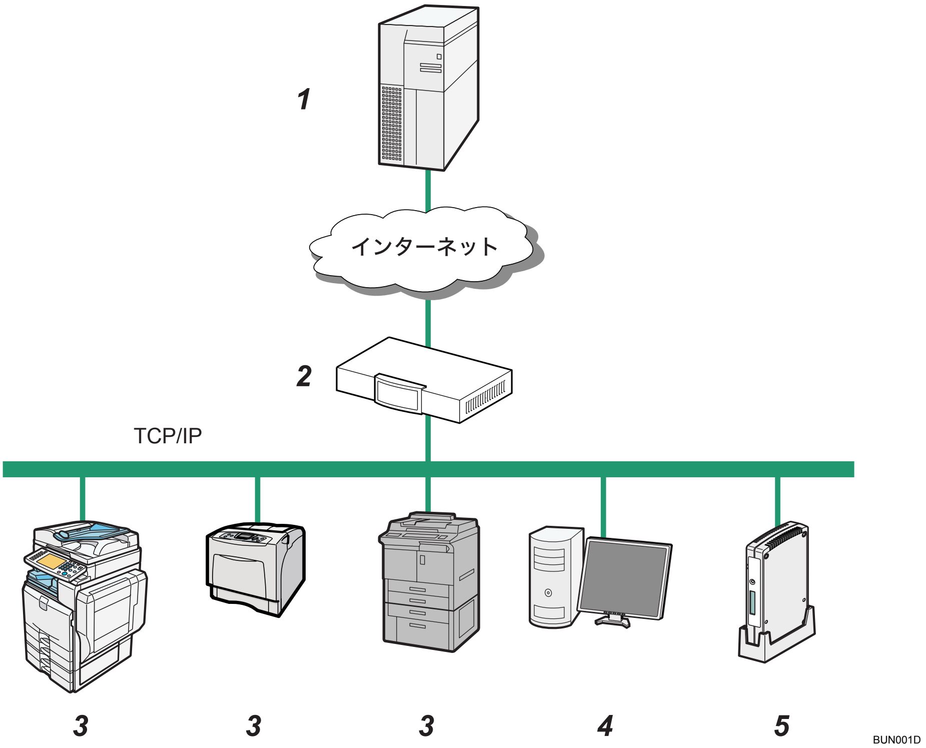
1

システム概要

本機は、インターネットを経由して HTTPS 接続で RS センターシステムと通信できます。HTTPS 接続で相互認証することで、本機と RS センターシステムとの通信の安全性が保障されます。RS センターシステムは HTTPS サーバーとして動作し、本機はクライアントとして機能します。

通信できるのは以下の条件を満たしている場合です。

- お使いのネットワーク環境が、外部の Web サイトにアクセスできる。
- プロキシ認証を用いる場合、本機のアカウントとパスワードが利用できる。



1. **RS センターシステム**

   各種サービスのための情報を集約するセンターです。

2. **プロキシサーバーおよびファイアウォール**

   プロキシサーバーやファイアウォールを使用できます。プロキシサーバーを使用する場合、「ベーシック認証」、「ダイジェスト認証」および「Windows 統合認証」（NTLMv2 認証だけ）を使用した環境に対応しています。

3. **デバイス**

   管理対象となるデバイスの種類は、デジタル複合機、プリンターです。本機には最大 100 台のデバイスを登録できます。

- 本機の管理対象となるデバイスには、HTTPS 対応機と SNMP 対応機の 2 種類があります。利用者は、機器登録ウィザードや登録機器一覧におけるデータ項目「機器接続方式」を確認することでその識別が可能です。
- 本機と HTTPS 対応機との通信は、HTTPS 接続で相互認証することで安全性が保証されます。HTTPS 対応機の設定に関する要件は、各デバイスの管理者設定項目の「@Remote サービス」が「禁止しない」に設定されていることです。
- 本機と SNMP 対応機との通信は、SNMPv1,v2 および SNMPv3 を使用できます。

オプションでメモリーおよびストレージを拡張すると、1,000 台まで登録できます。詳細は、サービス実施店にご相談ください。

オプションの詳細は、P.17「オプション名称とはたらき」を参照してください。

4. 管理用のパソコン

RC Gate モニターを使って、本機を管理します。RC Gate モニターの詳細は、P.18「RC Gate モニターについて」を参照してください。

5. 本機（RC Gate）

デバイスの各種情報を RS センターシステムへ通知したり、RS センターシステムからデバイスの更新用ソフトウェアをダウンロードしたりと、デバイスと RS センターシステムの仲介役を果たします。

メモリーを拡張すると RS センターシステムから指定されたデバイスのカウンター情報を、ユーザー別（ユーザーコード別）に収集して RS センターシステムに通知できます。ユーザー別カウンターを利用したサービスについての詳細は、サービス実施店にご相談ください。

オプションの詳細は、P.17「オプション名称とはたらき」を参照してください。

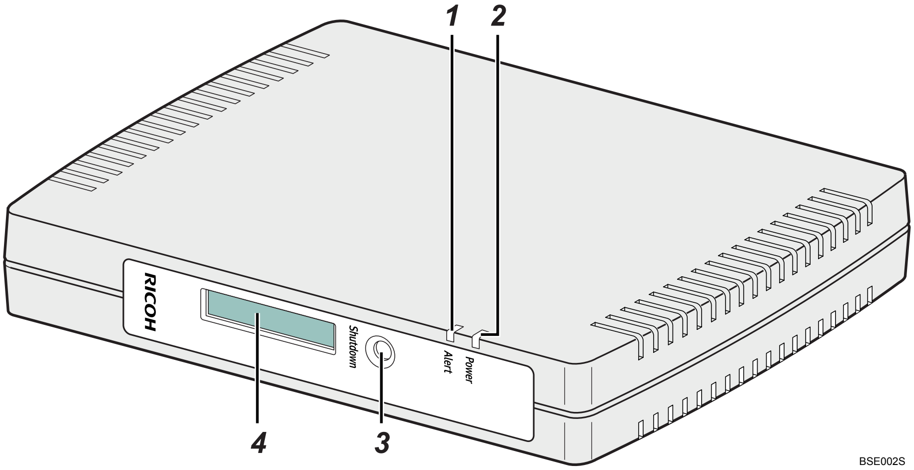
各部の名称とはたらき

各部の名称とはたらきについて説明します。

1

前面

前面の各部の名称とはたらきについて説明します。



1. **Alert（赤）**

   本機の状態によって表示パターンが異なります。

   - 証明書が発行されていないときに、点灯します。
   - 以下の場合、ゆっくり点滅します。
     - ユーザー設定によりサービスが休止しているとき
     - 通信エラーが発生しているとき
   - 以下の場合、高速で点滅します。
     - RS センターシステムとの通信が休止しているとき
     - システムエラーが発生しているとき
     - 異常が発生し、サービスが休止しているとき
   - RS センターシステムと正常に通信しているときは、消灯します。

2. **Power（緑）**

   通電時に点灯します。

3. **Shutdown ボタン**

   5 秒以上押し続けると、本機がシャットダウンします。

   電源プラグを抜く前にシャットダウンしないと、記憶媒体が破損する場合があります。その際、最新ログが最大で 1 時間分失われることがあります。電源プラグを抜く前に、必ずシャットダウンしてください。

4. 画面

1 行目に本機の状態を表示し、2 行目に本機の LAN ポートに設定された IP アドレスを表示します。

本機に異常が発生した場合、2 行目の表示がエラーコードに切り替わります。

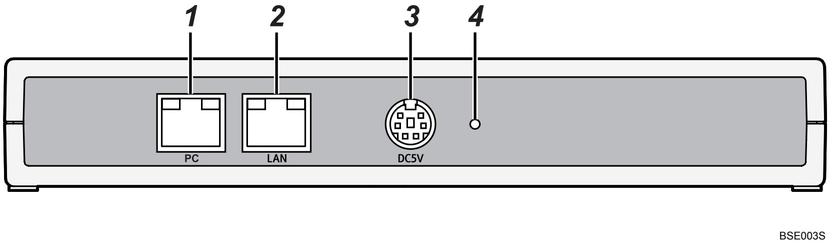
エラーコードの詳細は、P.139「RC Gate の画面に表示されるメッセージ」を参照してください。

補足

- 「Alert」LED が点滅したり、画面にエラーコードが表示されたりした場合は、P.141「こんなときには」を参照してください。
- 本機を再起動する場合は、P.122「RC Gate 再起動」を参照してください。

背面

背面の各部の名称とはたらきについて説明します。



1. PC ポート（メンテナンスポート）

カスタマーエンジニアがメンテナンスするときや、管理者が本機の初期設定および登録するときに使うポートです。

2. LAN ポート

本機をご利用のネットワークに接続するときに使うネットワーク（Ethernet）ポートです。

工場出荷時の IP アドレスは 192.168.0.2 ですが、変更可能です。

3. 電源コネクター

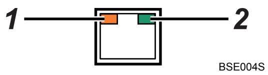
電源コードを接続するときに使うコネクターです。

4. ねじ穴

電源コード固定金具をねじ止めするときに使う穴です。

LAN ポートの LED

通電時、PC ポート（メンテナンスポート）および LAN ポートの接続状態が確認できます。



1

1. LED（接続状態）

本機がネットワークに接続しているときに点灯します（オレンジ色）。

2. LED（送受信状態）

データを送受信しているときに点灯します（緑色）。

オプション名称とはたらき

本機のオプションの名称とはたらきについて説明します。

本機では、ハードウェアオプションとしてメモリーおよびストレージの容量を拡張できます。設置については、サービス実施店にご相談ください。

- Remote Communication Gate Memory 1000

  標準 128 MB のメモリー容量を、512 MB に拡張できます。

- Remote Communication Gate Storage 1000

  標準 2 GB のストレージ容量を、18 GB に拡張できます。

補足

- 本機に登録できるデバイスは通常最大で 100 台ですが、オプションでメモリーおよびストレージを拡張すると 1,000 台まで登録できます。詳細は、サービス実施店にご相談ください。
- メモリーを拡張すると、RS センターシステムから指定されたデバイスのカウンター情報を、ユーザー別（ユーザーコード別）に収集して RS センターシステムに通知できます。ユーザー別カウンターを利用したサービスについての詳細は、サービス実施店にご相談ください。

RC Gate モニターについて

RC Gate モニターは、本機およびデバイスの登録や設定をしたり、状態を閲覧したりするためのソフトウェアです。RC Gate モニターは、本機に内蔵されており、同一ネットワーク上のパソコンの Web ブラウザーを使ってアクセスできます。

重要

- **以下の場合は、表示や操作に不具合が生じる可能性があります。**
    - **使用する Web ブラウザーのバージョンが推奨ブラウザーより低い。**
    - **「JavaScript」が有効になっていない。**
    - **「Cookie の使用許可」が有効になっていない。**
    - **キャッシュを表示する設定になっている。**
- **使用する Web ブラウザーの文字サイズの設定によっては、ページレイアウトが崩れる場合があります。文字サイズは「中」以下に設定することをお勧めします。**
- **お使いの Web ブラウザーが、表示言語に対応していない場合は、文字化けを起こす可能性があります。**

対象 OS

以下の推奨 Web ブラウザーをサポートする OS をご使用ください。

推奨 Web ブラウザー

Microsoft Internet Explorer 6.0 以降（IPv6 アドレスの URL でアクセスするときは、Internet Explorer 7.0 以降）

重要

- **あらかじめ Adobe Flash Player 10.0 以降をインストールしてください。**

補足

- SSL 通信で使用する証明書については、ネットワーク管理者にお問い合わせください。

RC Gate モニターのユーザー

本機にログインできるユーザーの種類は、以下のとおりです。

管理者

本機の設置やデバイスの登録、本機の設定変更、登録されたデバイスの管理情報の閲覧ができます。

管理者でログインするときは、表示する画面を「導入設定」画面と「RC Gate 情報確認/設定」画面から選択します。

「導入設定」画面を選択した場合は、以下のメニューが表示されます。

- セットアップウィザード

  本機を初期設定するためのウィザードを起動します。

  一度セットアップウィザードの設定を完了すると、次回から本メニューは表示されません。

- @Remote サービス登録ウィザード

  本機を RS センターシステムに照会・登録するためのウィザードを起動します。

  「セットアップウィザード」が完了している場合に表示されます。一度@Remote サービス登録を完了すると、次回から本メニューは表示されません。

- 機器ファームウェア更新時刻シフト

  ファームウェアの更新時刻を、ネットワークのセグメントごとに設定するためのウィザードを起動します。

  @Remote サービス登録が完了している場合に表示されます。

- 除外指定 IP アドレス設定

  本機からアクセスを禁止するデバイスの IP アドレスを指定するためのウィザードを起動します。

  @Remote サービス登録が完了している場合に表示されます。

- Ping 送信許可設定

  Ping の送信可否を設定するためのウィザードを起動します。

  @Remote サービス登録が完了している場合に表示されます。

- オートディスカバリー設定ウィザード

  オートディスカバリー機能の使用可否およびスケジュールを設定するためのウィザードを起動します。

  @Remote サービス登録が完了している場合に表示されます。

- 機器登録ウィザード

  デバイスを RS センターシステムに登録するためのウィザードが起動します。

  @Remote サービス登録が完了している場合に表示されます。

一般ユーザー

本機が管理するデバイスの責任者で、デバイスの情報や設定値の閲覧だけでき、本機の設定値を変更する権限はありません。最大 10 ユーザーの登録ができます。

一般ユーザーは、以下の画面を閲覧できます。

- 登録機器一覧

  RC Gate が管理するデバイスの一覧を表示します。

- 機器詳細

  RC Gate が管理するデバイスの詳細情報を表示します。

  コール通知履歴

コールを通知した日付、コール種別、コールが発生したデバイス情報を表示します。

- サービスコール

RC Gate に障害が発生した場合、エラーコード等の情報を表示します。

一般ユーザーでログインするためには、管理者による一般ユーザーのユーザーアカウント作成が必要です。詳細は、P.127「ユーザーアカウント設定」を参照してください。

補足

- 使用していない一般ユーザーのアカウントは、管理者に連絡し、削除してください。

RC Gate モニターを起動するには

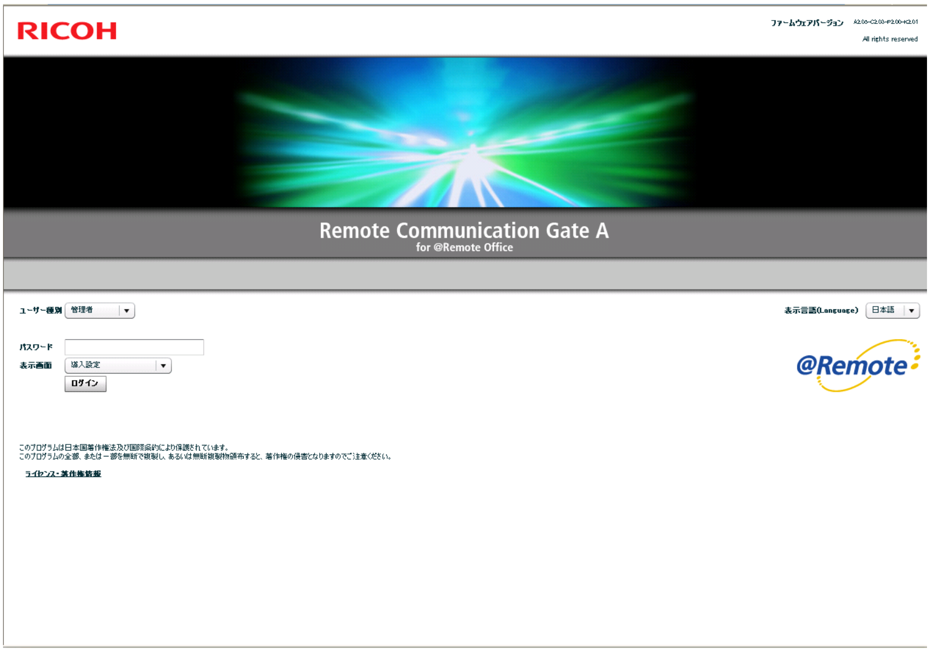
重要

- パスワードを入力する際、入力した文字を隠す機能（たとえば「*」などのダミー文字を表示）を持ったブラウザーを必ず使用してください。
- RC Gate モニターログイン時のパスワードは変更してください。工場出荷時のパスワードでは運用しないでください。詳細は、P.128「パスワード」を参照してください。
- セキュリティの観点から、5 分のあいだに 3 回ログインに失敗すると、本機へのログインが禁止になります。1 分後に再度ログインできます。

1. **同一ネットワーク上のパソコンの Web ブラウザーを起動する。**
2. **Web ブラウザーの URL 欄に、「https://{LAN ポートの IP アドレス}:9443/index.html」と入力する。**
3. **［はい］をクリックする。**
4. **ファームウェアバージョンが RC Gate モニターのトップページ右上に表示されます。セキュリティ認証(CC)を取得した製品として本機をご使用のお客様は、認証を取得したファームウェアバージョンであることをご確認ください。認証を取得したファームウェアバージョンはマニュアル入手先 URL にて確認できます。「表示言語(Language)」欄が［日本語］になっていることを確認し、「ユーザー種別」欄から、［管理者］または［一般ユーザー］のいずれかを選択し、対応するパスワード（半角文字）を入力する。**

   ［一般ユーザー］を選択した場合は、下記を行ってください。

   - 管理者が設定したパスワードを入力します。
   - 「ユーザー名」にユーザー名を入力します。



5. 表示画面を選択する。

6. ［ログイン］をクリックする。

補足

- RC Gate モニターにアクセスできない場合は、P.22「プロキシを設定する（Internet Explorer 6.0 の場合）」P.22「プロキシを設定する（Internet Explorer 6.0 の場合）」を参照して、プロキシを設定してください。
- RC Gate モニターにアクセスすると、セキュリティログに記録されます。詳細は、P.135「セキュリティログ」を参照してください。

ソフトウェアの正当性をチェックする

RC Gate モニターを操作する前に、RC Gate に内蔵されているソフトウェアが正規品かどうかチェックします。

1. RC Gate モニターを起動し、表示画面から［導入設定］を選択し、［管理者］でログインする。

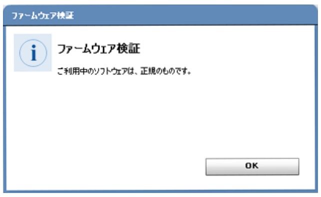
2. ［システムファームウェア検証］をクリックする。



チェック結果を示す画面が表示されます。

ソフトウェアが正規品でない場合は、「ご利用中のソフトウェアは、正規のものではありません。サービスに連絡し、指示に従ってください。」というメッセージが表示されます。画面の指示に従ってサービス実施店にご連絡ください。

3. ［OK］をクリックする。



トップページに戻ります。

プロキシを設定する（Internet Explorer 6.0 の場合）

以下の手順で、プロキシサーバーの設定をします。

1. Web ブラウザーの［ツール］メニューから［インターネットオプション］を選択する。
2. [接続]タブをクリックする。
3. [LAN の設定]をクリックする。

4. 「プロキシサーバー」の「LAN にプロキシサーバーを使用する（これらの設定はダイヤルアップまたは VPN 接続には適用されません）」を選択し、[詳細設定]をクリックする。

5. 「例外」の「次で始まるアドレスにはプロキシを使用しない」に、本機の LAN ポートの IP アドレスを入力する。

6. [OK]を３回クリックする。

RC Gate モニターを終了するには

重要

- Web ブラウザーを終了する前に、管理者/一般ユーザーは必ず［ログアウト］をクリックしてください。［ログアウト］をクリックする前に Web ブラウザーを閉じると、RC Gate モニターにログインしたままになります。
- 操作を終了するときは［ログアウト］をクリックしてください。ログインしたまま５分間無操作の状態が続くと自動的にログアウトされます。

1. ヘッダーエリアの［ログアウト］をクリックする。

2. ログインユーザーが RC Gate モニターからログアウトしたことを確認し、Web ブラウザーを終了する。

2. 本機・デバイスを RS センターシステムに登録する

ここでは、本機およびデバイスを RS センターシステムに登録する手順について説明します。

まず、「@Remote サービス登録ウィザード」を使って本機を RS センターシステムに照会・登録します。

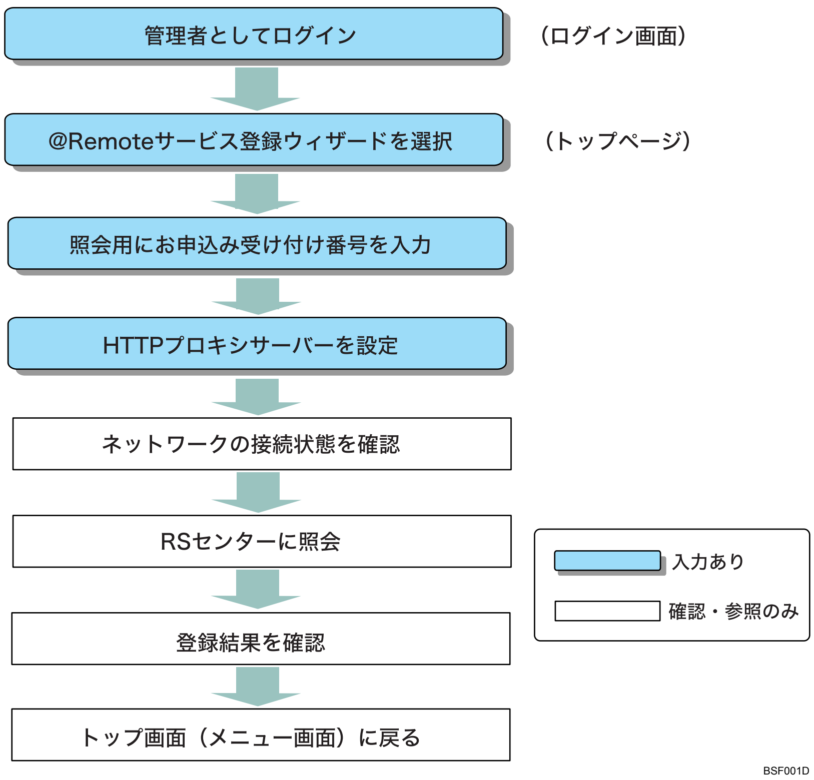
次に、「機器登録ウィザード」を使って、デバイスを RS センターシステムに照会・登録します。

「機器登録ウィザード」は、管理者でログインしていて、なおかつ「@Remote サービス登録ウィザード」が終了している場合に表示されるメニューです。

画面の操作方法は、P.18「RC Gate モニターについて」を参照してください。

@Remote サービス登録ウィザードの流れ

ここでは、本機を RS センターシステムに登録する流れについて説明します。



@Remote サービス登録ウィザードの操作手順

ここでは、本機を RS センターシステムに登録する手順について説明します。

2

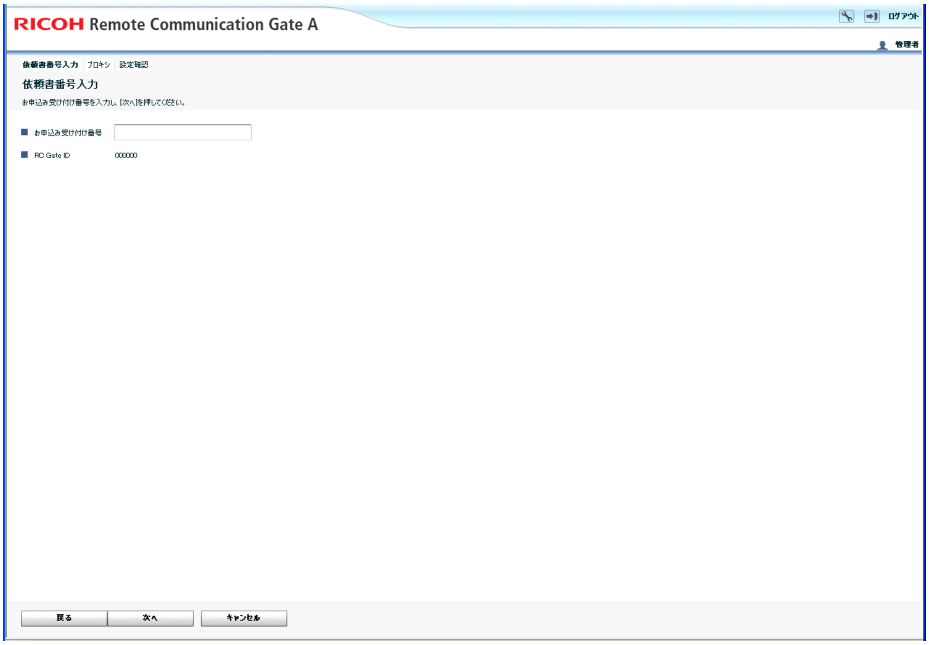
1. **Web ブラウザーを起動して RC Gate モニターを起動し、[管理者] でログインする。**

   RC Gate モニターの起動については、P.20「RC Gate モニターを起動するには」を参照してください。

2. **[@Remote サービス登録ウィザード] をクリックする。**

   一度登録を完了すると [@Remote サービス登録ウィザード] は表示されません。P.30「機器登録ウィザードの操作手順」に進んでください。

3. **「お申込み受け付け番号」を入力し、[次へ] をクリックする。**

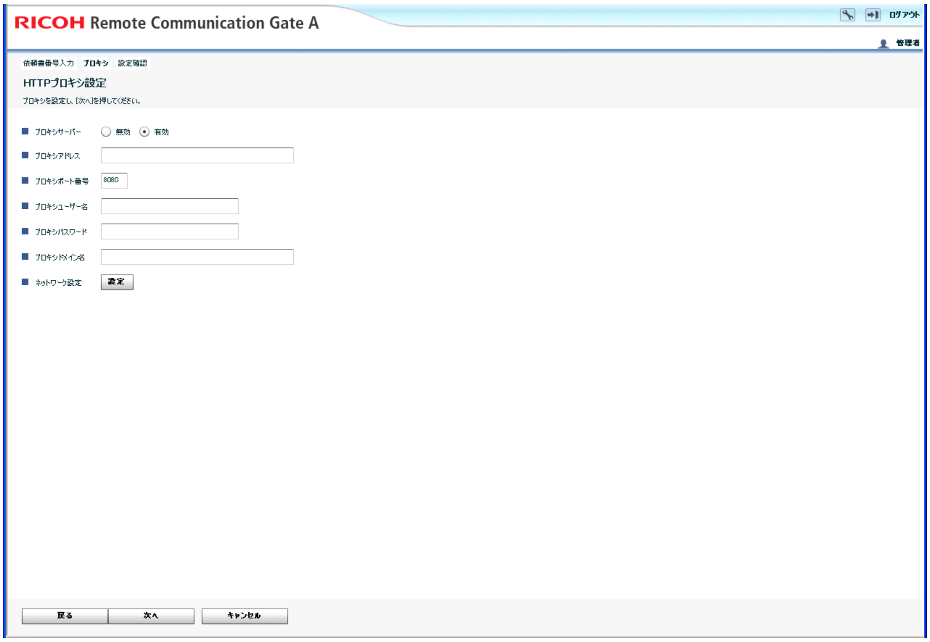
   「お申込み受け付け番号」欄には、『@Remote 設定依頼書』の「お申込み受け付け番号」を入力します。「お申込み受け付け番号」は RS センターシステム照会時のキーとなるため、入力が必須です。

   デバイスが複数台ある場合は、そのうちの 1 台の「お申込み受け付け番号」を入力してください。

4. **HTTP プロキシサーバーを使用する場合は「プロキシサーバー」を [有効] にしてプロキシを設定し、[次へ] をクリックする。**

   ネットワーク設定を変更する場合は、[設定] をクリックします。

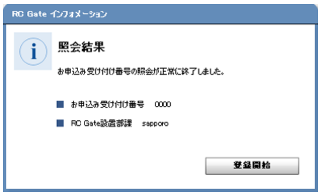
HTTP プロキシサーバーを使用しない場合は、［無効］を選択し、［次へ］をクリックします。



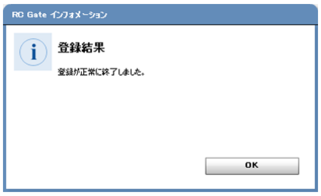
5. 接続状態を確認して、［次へ］をクリックする。

RS センターシステムへの照会作業には数分かかります。「照会結果」画面が表示されるまでお待ちください。

6. 正常に照会されたことを確認し、［登録開始］をクリックする。



7. 正常に登録されたことを確認し、［OK］をクリックする。



「@Remote サービス登録ウィザード」が終了し、「導入設定」画面に戻ります。

続いて、「機器登録ウィザード」を起動し、デバイスを RS センターシステムに登録します。

デバイスの登録手順は、P.30「機器登録ウィザードの操作手順」を参照してください。

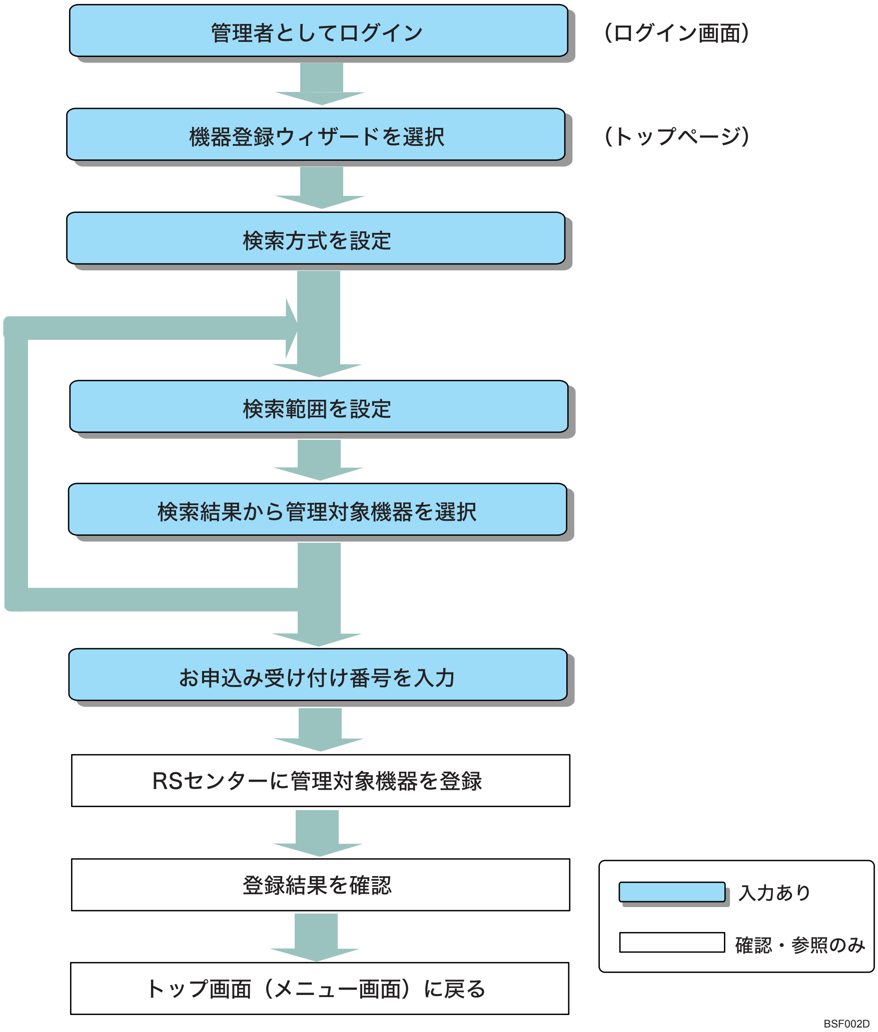
8. PC ポートにネットワークケーブルを接続している場合は、PC ポートからネットワークケーブルを抜き、パソコンのネットワーク設定を元に戻す。

補足

- 照会に失敗したときは、［OK］が表示されます。［OK］をクリックして、手順 3 からやり直してください。

機器登録ウィザードの流れ

ここでは、デバイスを RS センターシステムに登録する流れについて説明します。



機器登録ウィザードの操作手順

ここでは、ネットワーク上のデバイスを RS センターシステムに登録する方法を説明します。

登録するデバイスの検索範囲は、以下の 5 つの方法から選択できます。

- IPv4 アドレスの範囲を指定して検索する。
- ホスト名を指定して検索する。
- ネットワークのセグメントを指定して検索する。
- IPv6 アドレスを指定して検索する。
- IPv6 アドレスをマルチキャスト検索する。

重要

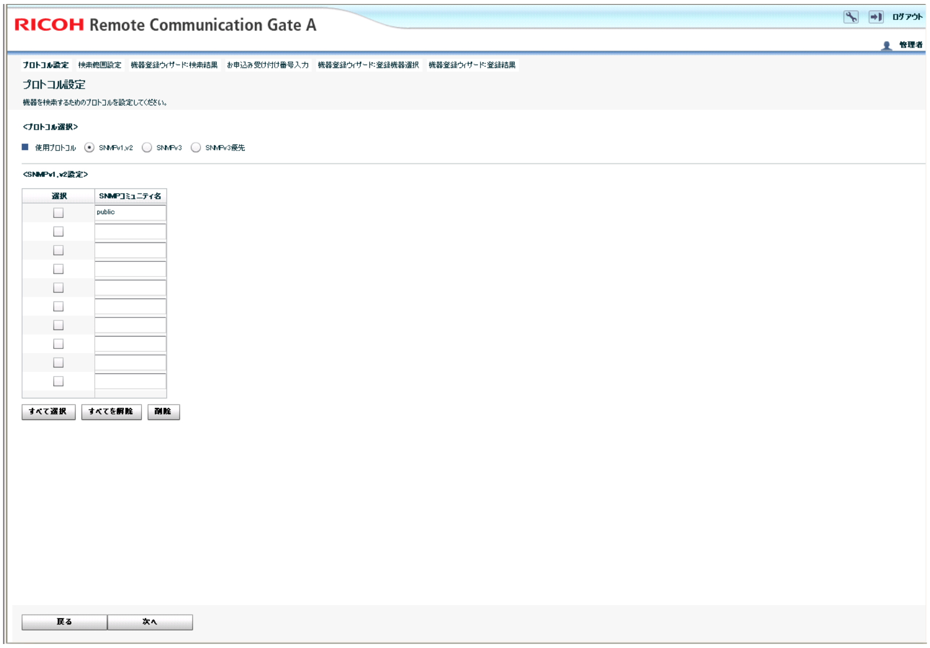
- 本機に登録できるデバイスは通常最大で 100 台ですが、オプションでメモリーおよびストレージを拡張すると 1,000 台まで登録できます。詳細は、サービス実施店にご相談ください。
- パソコンに保存された CSV ファイルからも検索範囲をインポートできます。詳細は P.54「CSV ファイルを作成する」を参照してください。

IPv4 アドレス範囲を指定してデバイスを検索する場合

登録するデバイスの検索範囲を、デバイスの IPv4 アドレスで指定する方法を説明します。

1. **RC Gate モニターが起動していない場合は起動し、[管理者] でログインする。**
2. **[機器登録ウィザード] をクリックする。**

3. 検索に使用する SNMP プロトコルを選択し、［次へ］をクリックする。



- ［SNMPv1,v2］を選択した場合：

  SNMP コミュニティ名を、1 件以上入力します（ASCII 文字 30 字以内で最大 10 件）。複数入力する場合は、使用頻度が高い順に入力します。

  使用していない SNMP コミュニティ名は削除してください。

  SNMP コミュニティ名は、本機が SNMP 対応機にアクセスするときにパスワードのような働きをします。詳細は、各デバイスの取扱説明書を参照してください。

  デバイスが HTTPS 対応機だけの場合は、SNMP コミュニティ名の入力は不要です。

- ［SNMPv3］を選択した場合：

  ユーザー名、認証用パスワード、暗号化パスワードを 1 セット以上入力します。最大 10 件入力できます。

- ［SNMPv3 優先］を選択した場合：

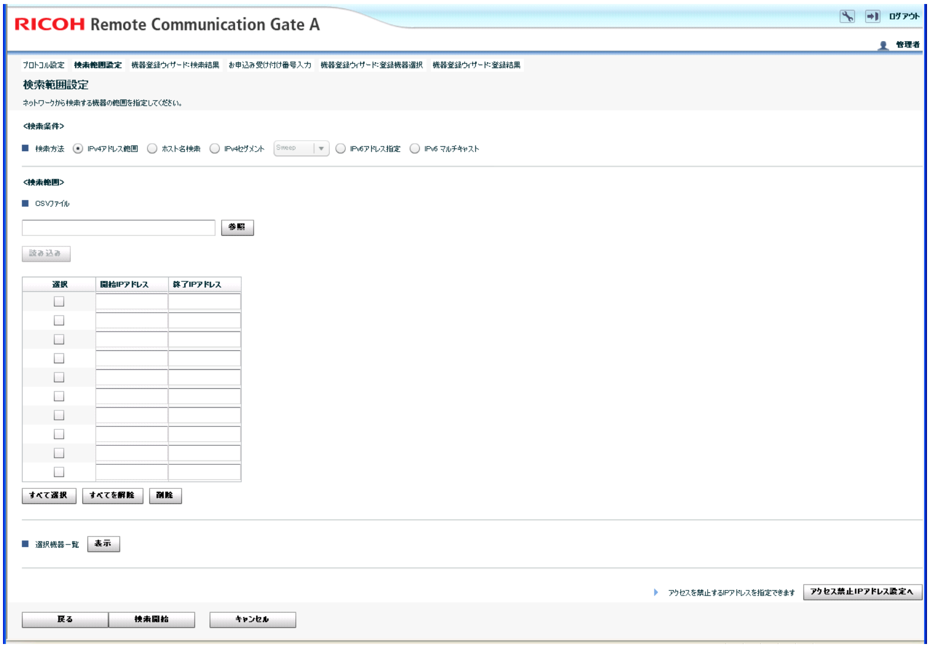
  SNMPv3 と SNMPv1,v2 プロトコルを使用します。最初に SNMPv3 プロトコルを使用して、デバイスを検索します。デバイスが SNMPv3 対応でない場合、SNMPv1,v2 プロトコルを使用して検索します。

リスト内の項目をすべて選択する場合は、［すべて選択］をクリックします。

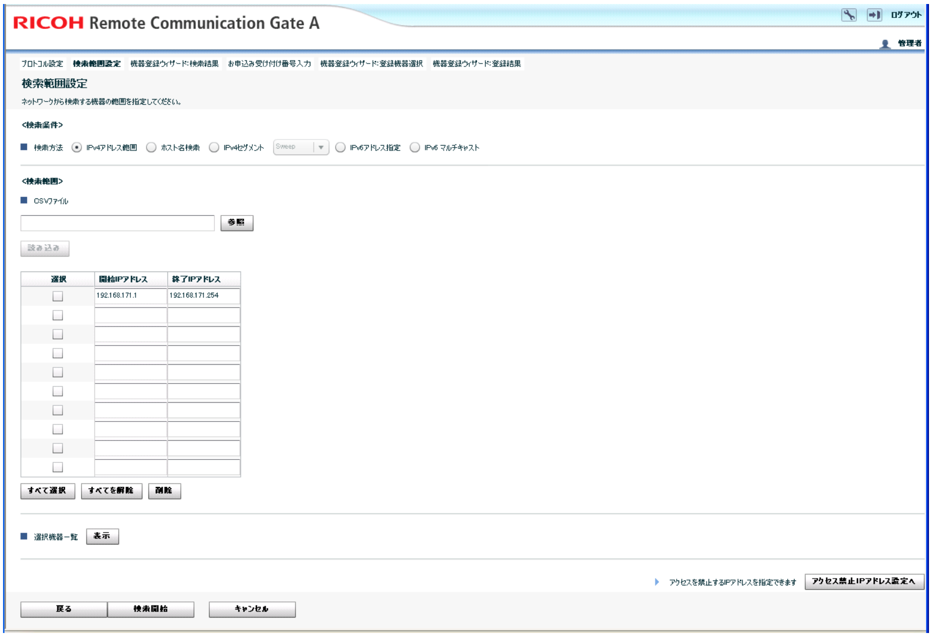
項目の選択をすべて解除する場合は、［すべてを解除］をクリックします。

2

4. 検索方法を［IPv4 アドレス範囲］に設定する。



5. 検索範囲を設定する。



- 直接入力する場合：

  検索開始 IPv4 アドレスと検索終了 IPv4 アドレスを「x. x. x. x」形式（「x」は 0～255 の範囲内の整数）で入力します。最大 10 件入力できます。

終了 IPv4 アドレスは、開始 IPv4 アドレスより大きな値を入力します。

検索終了 IPv4 アドレスに「0.0.0.0」を設定した行は検索されません。

検索開始 IPv4 アドレスに「0.0.0.0」を設定し、検索終了 IPv4 アドレスに「0.0.0.0」以外を設定した場合は検索エラーになります。

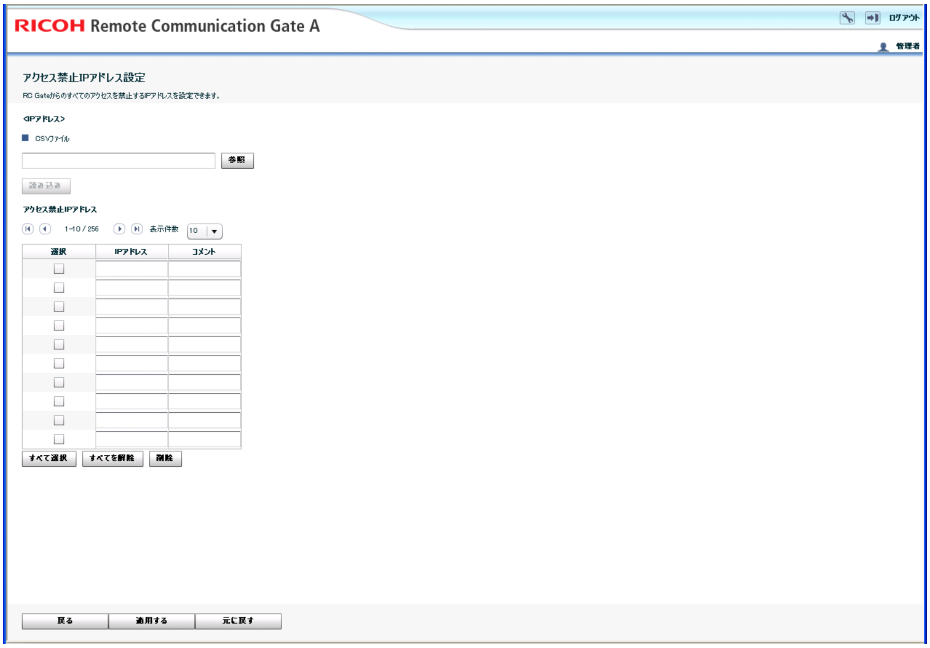
- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた検索範囲は削除されます。

6. ［アクセス禁止 IP アドレス設定へ］をクリックし、RC Gate からアクセスを禁止するデバイスの IPv4 アドレスを指定する。

アクセスを禁止する IPv4 アドレスを指定しない場合は、手順 8 に進んでください。



- 直接入力する場合：

  IPv4 アドレスを「x. x. x. x」形式（「x」は 0〜255 の範囲内の整数）で入力します。最大 256 件入力できます。

- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた IP アドレスは削除されます。

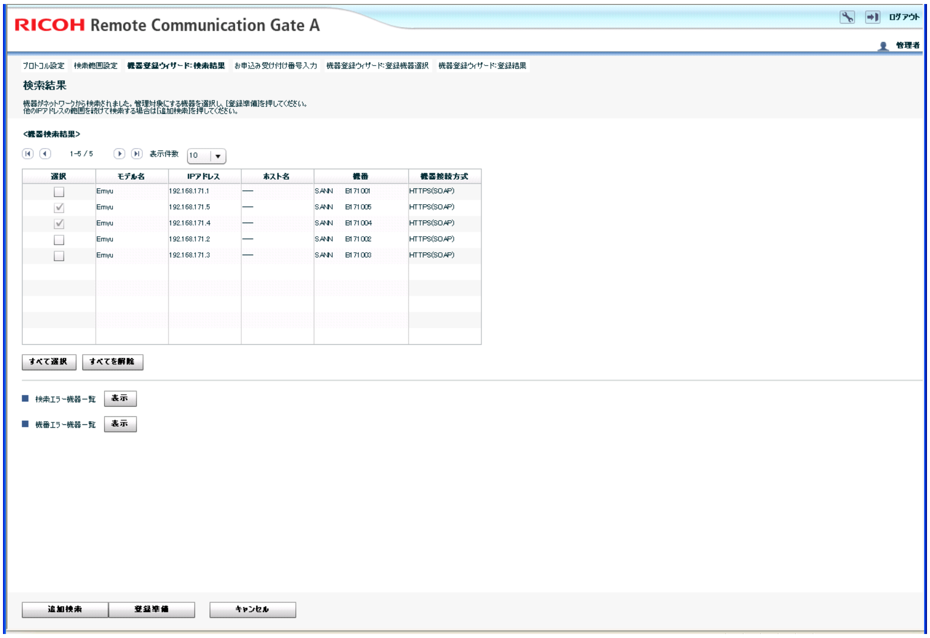
7. **アクセスを禁止したい IPv4 アドレスのチェックボックスを選択し、[OK] をクリックする。**

「検索範囲設定」画面に戻ります。

8. **[検索開始] をクリックする。**

デバイスの検索が始まります。

9. **検索されたデバイスの中から、登録したいデバイスのチェックボックスを選択し、[登録準備] をクリックする。**



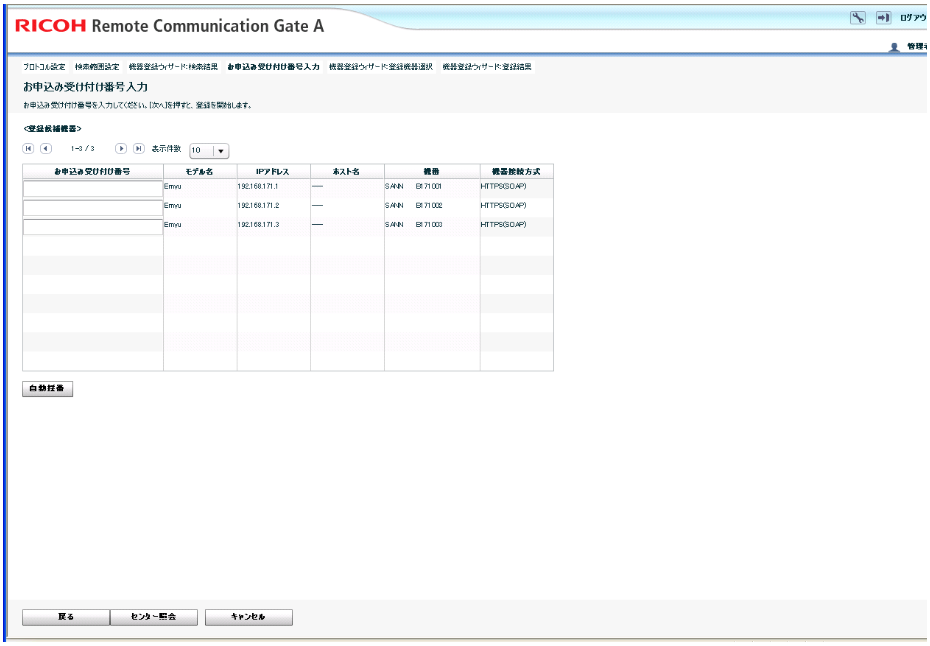
表示ページは、件数表示の左右にあるボタンをクリックして切り替えられます。 1 ページに表示する件数は、「表示件数」リストで変更できます。

登録済みデバイスは、[選択] 欄がマスク（灰色表示）されます。

- [すべて選択]：現在のページに表示されていないデバイスを含め、検索されたすべてのデバイスを選択します。
- [すべてを解除]：現在のページに表示されていないデバイスを含め、項目の選択をすべて解除します。
- [追加検索]：検索範囲を変更し、検索を繰り返します。手順 5 に戻って、検索範囲を設定してください。
- [機番エラー一覧]：本機が機番を識別できないデバイスの IP アドレス、MAC アドレス、モデル名の一覧を表示します。

10. **各デバイスの「お申込み受け付け番号」を入力し、[センター照会] をクリックする。**

「お申込み受け付け番号」を自動採番する場合は、[自動採番] をクリックします。



11. **RSセンターシステムに登録したいデバイスのチェックボックスを選択し、[登録]をクリックする。**

各デバイスの機番をクリックすると、照会されたデバイスの詳細情報を確認できます。同一モデルを複数台ご利用の場合は、各デバイスの設置場所を確認してください。

RSセンターシステムへの照会に失敗した場合は、「照会結果」欄に「NG」と表示されます。デバイスの機番をクリックして、詳細画面の「照会結果」欄に表示されている対処方法を確認してください。

12. **登録結果を確認し、[終了]をクリックする。**

「導入設定」画面に戻ります。

補足

- アクセスを禁止するIPv4アドレスは、本ウィザード終了後にも設定できます。詳細は、P.99「アクセス禁止IPアドレス」を参照してください。

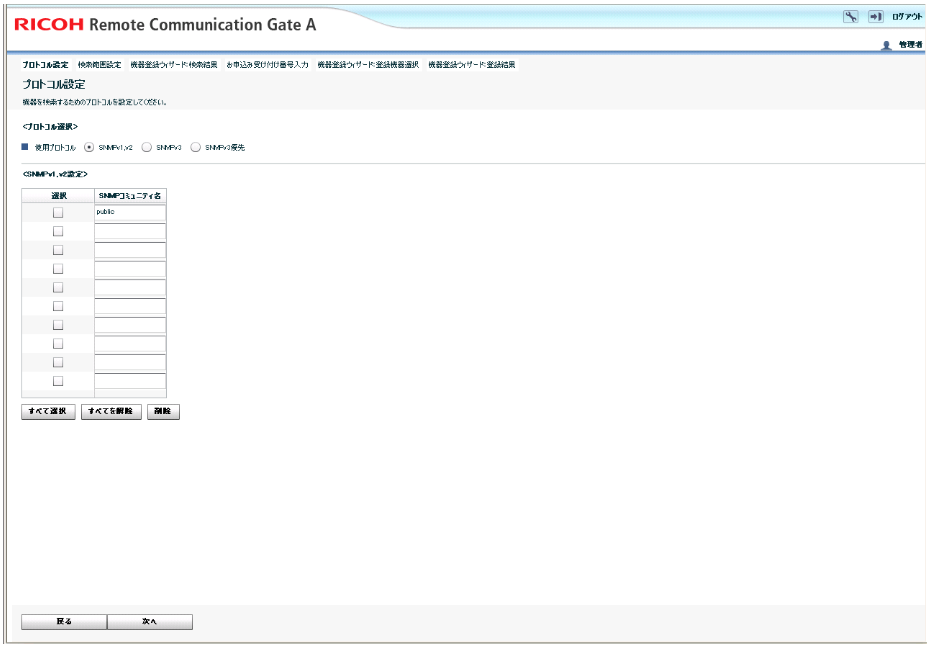
ホスト名を指定してデバイスを検索する場合

登録するデバイスの検索範囲を、ホスト名で指定する方法を説明します。

1. **RC Gateモニターが起動していない場合は起動し、[管理者]でログインする。**

2. **[機器登録ウィザード]をクリックする。**

3. 検索に使用する SNMP プロトコルを選択し、［次へ］をクリックする。



- ［SNMPv1,v2］を選択した場合：

  SNMP コミュニティ名を、1 件以上入力します（ASCII 文字 30 字以内で最大 10 件）。複数入力する場合は、使用頻度が高い順に入力します。

  使用していない SNMP コミュニティ名は削除してください。

  SNMP コミュニティ名は、本機が SNMP 対応機にアクセスするときにパスワードのような働きをします。詳細は、各デバイスの取扱説明書を参照してください。

  デバイスが HTTPS 対応機だけの場合は、SNMP コミュニティ名の入力は不要です。

- ［SNMPv3］を選択した場合：

  ユーザー名、認証用パスワード、暗号化パスワードを 1 セット以上入力します。最大 10 件入力できます。

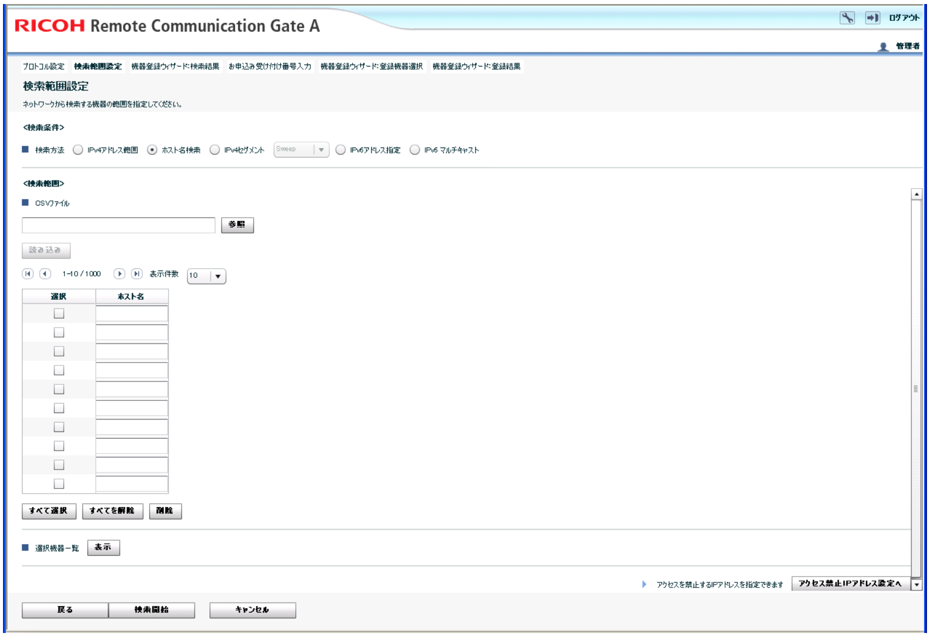
- ［SNMPv3 優先］を選択した場合：

  SNMPv3 と SNMPv1,v2 プロトコルを使用します。最初に SNMPv3 プロトコルを使用して、デバイスを検索します。デバイスが SNMPv3 対応でない場合、SNMPv1,v2 プロトコルを使用して検索します。

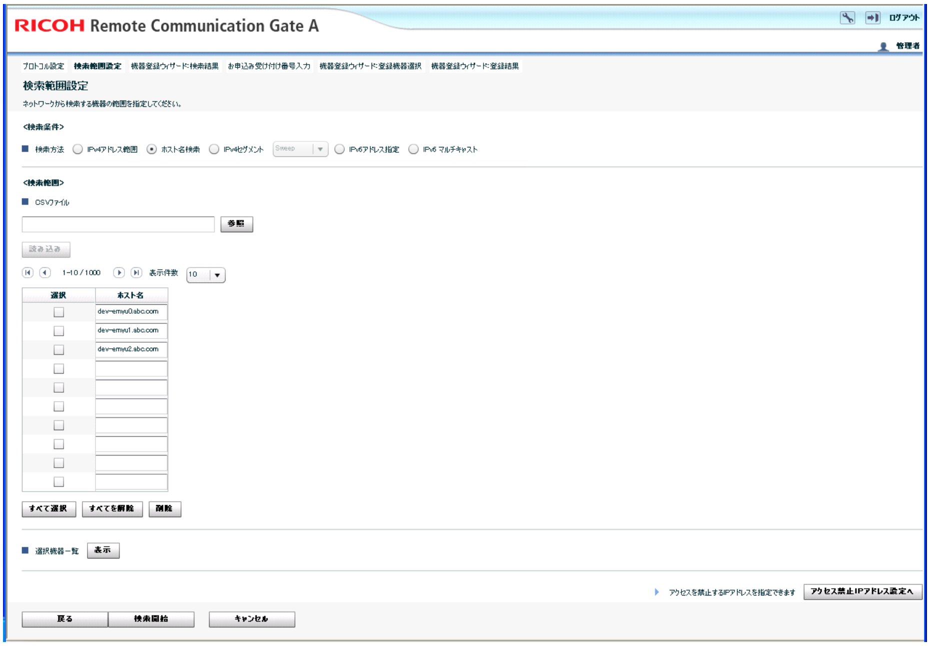
リスト内の項目をすべて選択する場合は、［すべて選択］をクリックします。

項目の選択をすべて解除する場合は、［すべてを解除］をクリックします。

4. 検索方法を［ホスト名検索］に設定する。



5. 検索範囲を設定する。



- 直接入力する場合：

  ホスト名を入力します。最大 100 件（オプションでメモリーおよびストレージを拡張すると 1,000 件）入力できます。

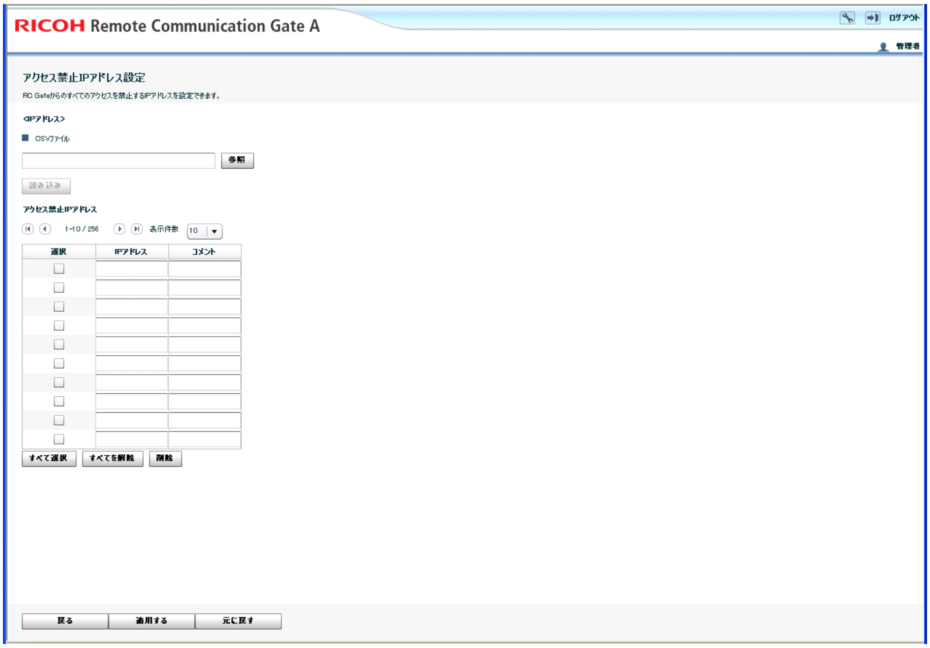
- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた IPv4 アドレスは削除されます。

6. ［アクセス禁止 IP アドレス設定へ］をクリックし、RC Gate からアクセスを禁止するデバイスの IPv4 アドレスを指定する。

アクセスを禁止する IPv4 アドレスを指定しない場合は、手順 8 に進んでください。



- 直接入力する場合：

  IPv4 アドレスを「x. x. x. x」形式（「x」は 0〜255 の範囲内の整数）で入力します。最大 256 件入力できます。

- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた IPv4 アドレスは削除されます。

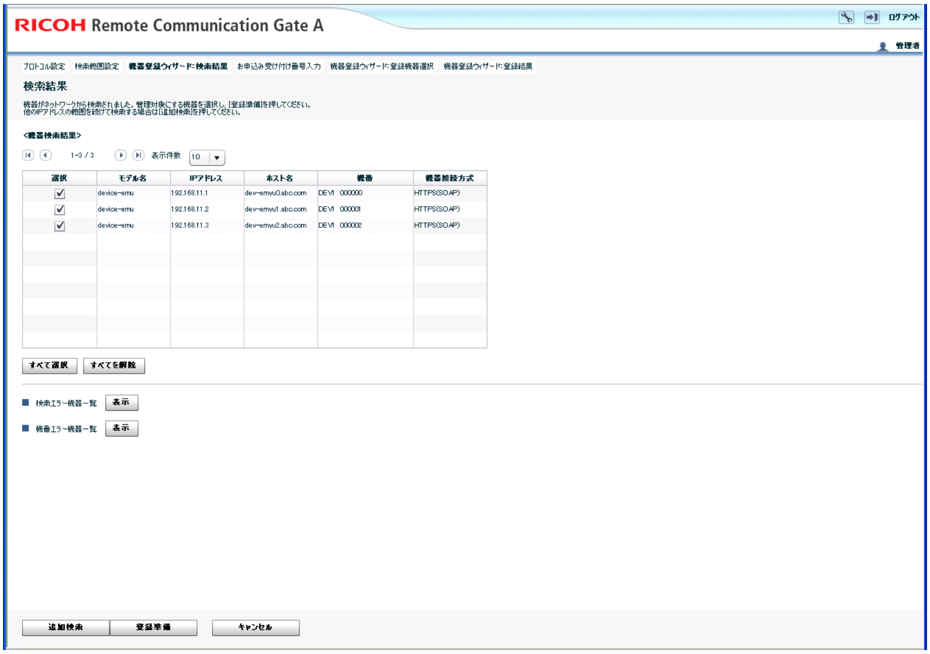
7. アクセスを禁止したい IPv4 アドレスのチェックボックスを選択し、［OK］をクリックする。

「検索範囲設定」画面に戻ります。

8. **[検索開始]をクリックする。**

デバイスの検索が始まります。

9. **検索されたデバイスの中から、登録したいデバイスのチェックボックスを選択し、[登録準備]をクリックする。**



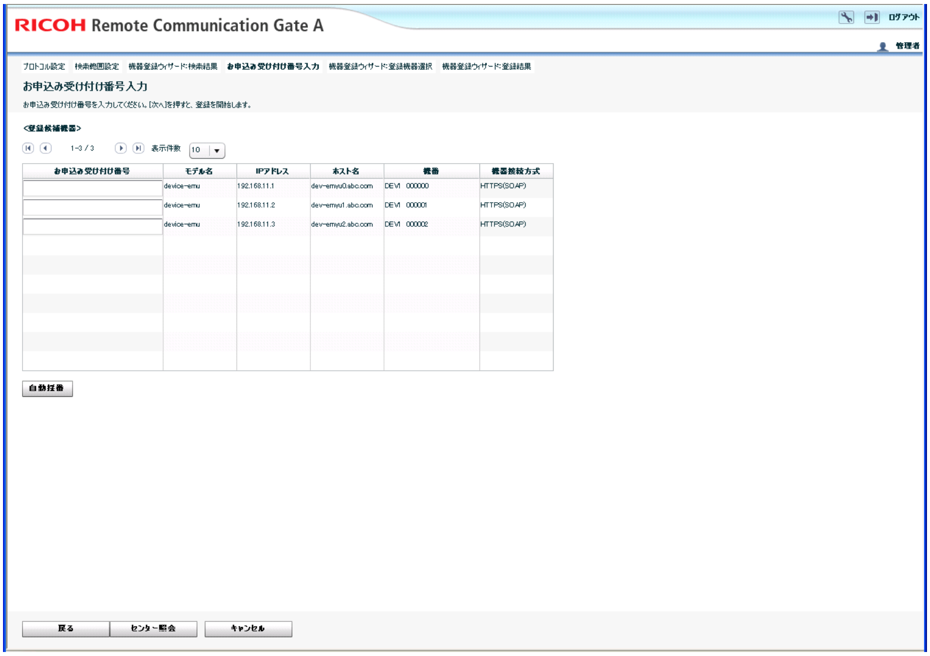
表示ページは、件数表示の左右にあるボタンをクリックして切り替えられます。1ページに表示する件数は、「表示件数」リストで変更できます。

登録済みデバイスは、[選択]欄がマスク(灰色表示)されます。

- [すべて選択]:現在のページに表示されていないデバイスを含め、検索されたすべてのデバイスを選択します。
- [すべてを解除]:現在のページに表示されていないデバイスを含め、項目の選択をすべて解除します。
- [追加検索]:検索範囲を変更し、検索を繰り返します。手順 5 に戻って、検索範囲を設定してください。
- [検索失敗一覧]:検索されたなったホスト名と IP アドレスを表示します。
- [機番エラー一覧]:本機が機番を識別できないデバイスの IP アドレス、MAC アドレス、モデル名の一覧を表示します。

10. **各デバイスの「お申込み受け付け番号」を入力し、[センター照会]をクリックする。**

「お申込み受け付け番号」を自動採番する場合は、[自動採番]をクリックします。



11. **RS センターシステムに登録したいデバイスのチェックボックスを選択し、［登録］をクリックする。**

機番をクリックすると、照会されたデバイスの詳細情報を確認できます。同一モデルを複数台ご利用の場合は、各デバイスの設置場所を確認してください。

RS センターシステムへの照会に失敗した場合は、「照会結果」欄に「NG」と表示されます。デバイスの機番をクリックして、詳細画面の「照会結果」欄に表示されている対処方法を確認してください。

12. **登録結果を確認し、［終了］をクリックする。**

「導入設定」画面に戻ります。

補足

- アクセスを禁止する IPv4 アドレスは、本ウィザード終了後にも設定できます。詳細は、P.99「アクセス禁止 IP アドレス」を参照してください。

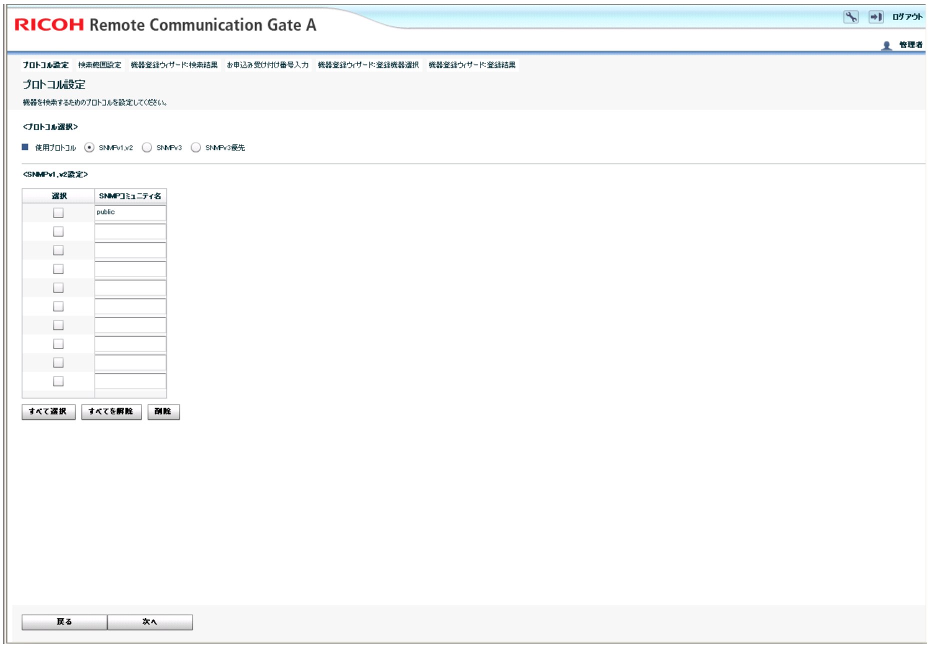
セグメントを指定してデバイスを検索する場合

登録するデバイスの検索範囲を、ネットワークのセグメントで指定する方法を説明します。

1. **RC Gate モニターが起動していない場合は起動し、［管理者］でログインする。**

2. **［機器登録ウィザード］をクリックする。**

3. 検索に使用するSNMPプロトコルを選択し、[次へ]をクリックする。



- [SNMPv1,v2]を選択した場合：

  SNMPコミュニティ名を、1件以上入力します（ASCII文字30字以内で最大10件）。複数入力する場合は、使用頻度が高い順に入力します。

  使用していないSNMPコミュニティ名は削除してください。

  SNMPコミュニティ名は、本機がSNMP対応機にアクセスするときにパスワードのような働きをします。詳細は、各デバイスの取扱説明書を参照してください。

  デバイスがHTTPS対応機だけの場合は、SNMPコミュニティ名の入力は不要です。

- [SNMPv3]を選択した場合：

  ユーザー名、認証用パスワード、暗号化パスワードを1セット以上入力します。最大10件入力できます。

- [SNMPv3優先]を選択した場合：

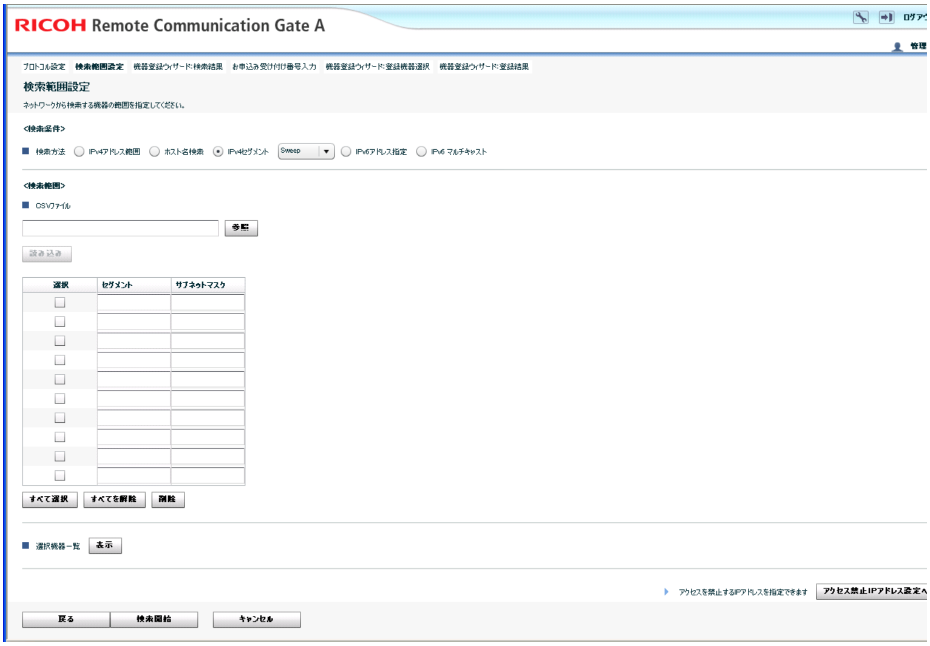
  SNMPv3とSNMPv1,v2プロトコルを使用します。最初にSNMPv3プロトコルを使用して、デバイスを検索します。デバイスがSNMPv3対応でない場合、SNMPv1,v2プロトコルを使用して検索します。

リスト内の項目をすべて選択する場合は、[すべて選択]をクリックします。

項目の選択をすべて解除する場合は、[すべてを解除]をクリックします。

2

4. 検索方法を［IPv4 セグメント］に設定し、検索手段を選択する。



検索手段は、以下から選択します。

- Sweep によるセグメント検索：

  指定したネットワークセグメントのすべての IPv4 アドレス（ホストアドレス 1～254）に対して、RC Gate が Ping を送信して検索します。

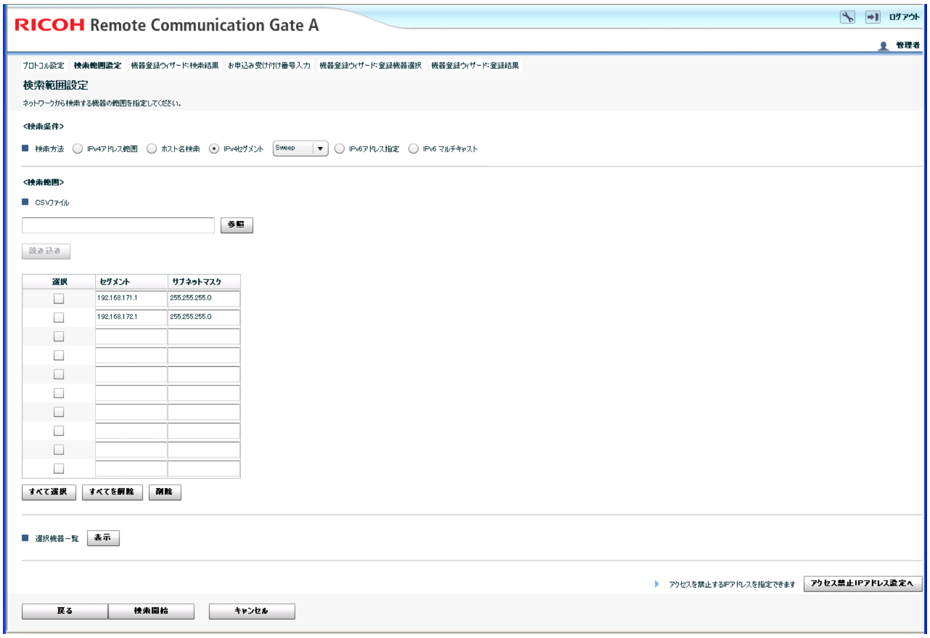
- BroadCast によるセグメント検索：

  指定したネットワークセグメントのブロードキャストアドレスに SNMP をブロードキャストして、応答があった IPv4 アドレスだけを検索します。

リスト内の項目をすべて選択する場合は、［すべて選択］をクリックします。

項目の選択をすべて解除する場合は、［すべてを解除］をクリックします。

5. 検索範囲を設定する。



- 直接入力する場合：

  セグメント情報として検索範囲とサブネットマスクを入力します。最大 10 件入力できます。

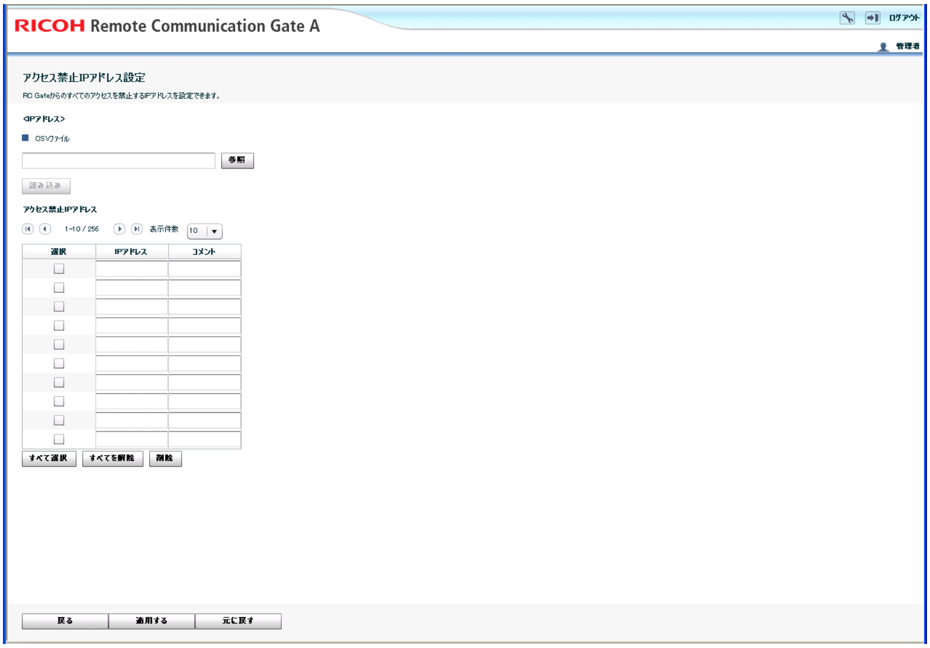
- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルからセグメント情報をインポートすると、インポート前に入力していた検索範囲は削除されます。

6. ［アクセス禁止 IP アドレス設定へ］をクリックし、RC Gate からアクセスを禁止するデバイスの IPv4 アドレスを指定する。

アクセスを禁止する IPv4 アドレスを指定しない場合は、手順 8 に進んでください。



- 直接入力する場合：

  IPv4 アドレスを「x. x. x. x」形式（「x」は 0〜255 の範囲内の整数）で入力します。最大 256 件入力できます。

- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた IPv4 アドレスは削除されます。

7. アクセスを禁止したい IPv4 アドレスのチェックボックスを選択し、［OK］をクリックする。

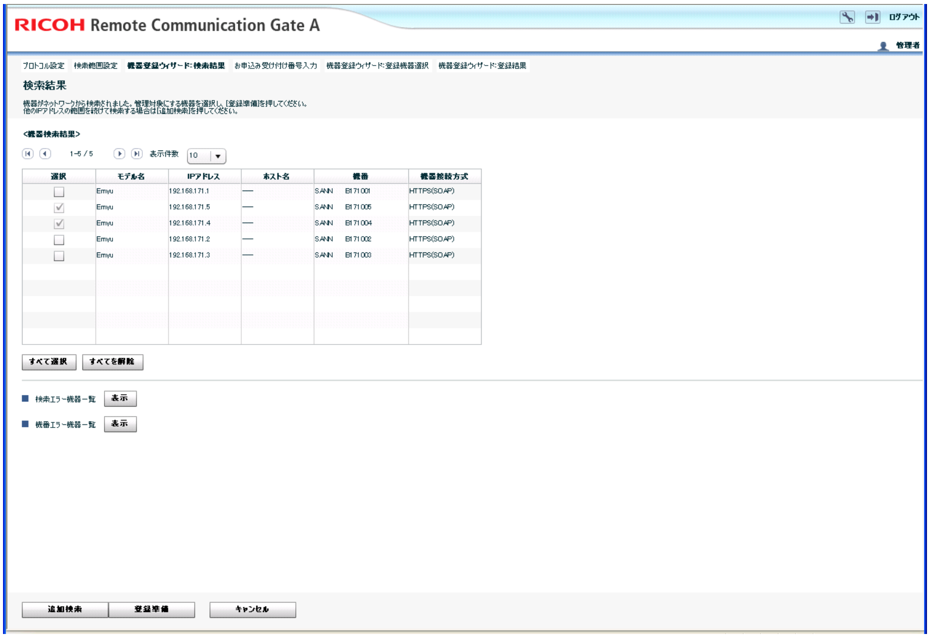
「検索範囲設定」画面に戻ります。

8. ［検索開始］をクリックする。

デバイスの検索が始まります。

2

9. **検索されたデバイスの中から、登録したいデバイスのチェックボックスを選択し、［登録準備］をクリックする。**



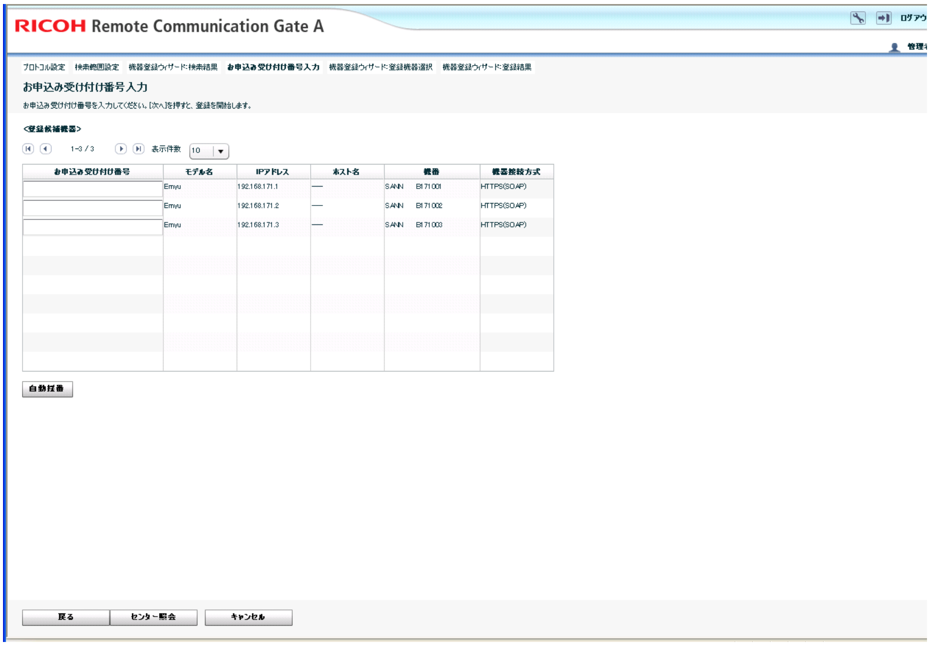
表示ページは、件数表示の左右にあるボタンをクリックして切り替えられます。1 ページに表示する件数は、「表示件数」リストで変更できます。

登録済みデバイスは、［選択］欄がマスク（灰色表示）されます。

- ［すべて選択］：現在のページに表示されていないデバイスを含め、検索されたすべてのデバイスを選択します。
- ［すべてを解除］：現在のページに表示されていないデバイスを含め、項目の選択をすべて解除します。
- ［追加検索］：検索範囲を変更し、検索を繰り返します。手順 5 に戻って、検索範囲を設定してください。
- ［機番エラー一覧］：本機が機番を識別できないデバイスの IP アドレス、MAC アドレス、モデル名の一覧を表示します。

10. **各デバイスの「お申込み受け付け番号」を入力し、［センター照会］をクリックする。**

「お申込み受け付け番号」を自動採番する場合は、［自動採番］をクリックします。



11. RS センターシステムに登録したいデバイスのチェックボックスを選択し、［登録］をクリックする。

機番をクリックすると、照会されたデバイスの詳細情報を確認できます。同一モデルを複数台ご利用の場合は、各デバイスの設置場所を確認してください。

RS センターシステムへの照会に失敗した場合は、「照会結果」欄に「NG」と表示されます。デバイスの機番をクリックして、詳細画面の「照会結果」欄に表示されている対処方法を確認してください。

12. 登録結果を確認し、［終了］をクリックする。

「導入設定」画面に戻ります。

補足

- アクセスを禁止する IPv4 アドレスは、本ウィザード終了後にも設定できます。詳細は、P.99「アクセス禁止 IP アドレス」を参照してください。

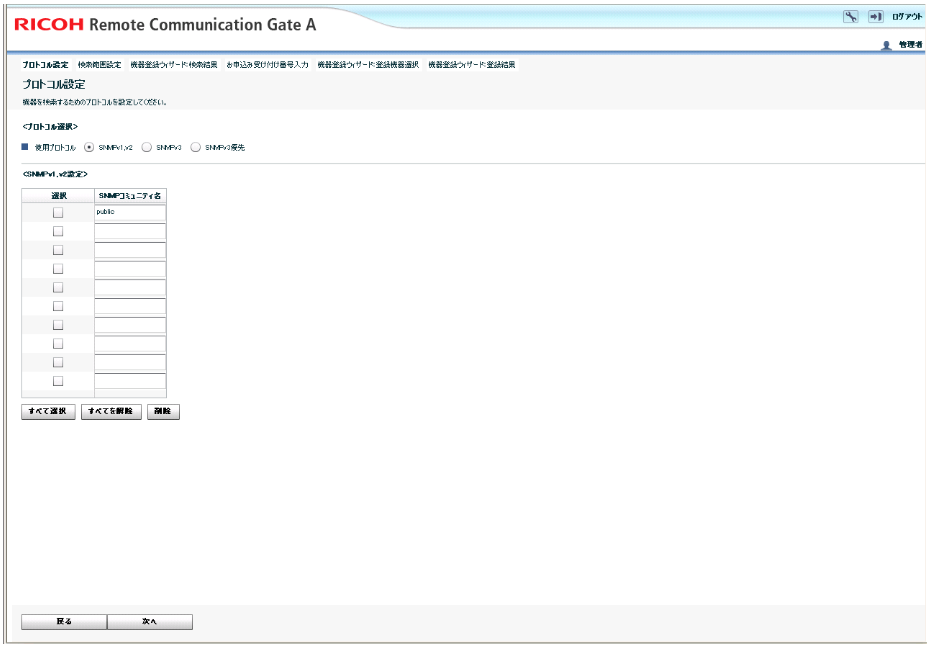
IPv6 アドレスを指定してデバイスを検索する場合

登録するデバイスの検索範囲を、デバイスの IPv6 アドレスで指定する方法を説明します。

1. RC Gate モニターが起動していない場合は起動し、［管理者］でログインする。

2. ［機器登録ウィザード］をクリックする。

3. 検索に使用する SNMP プロトコルを選択し、［次へ］をクリックする。



- ［SNMPv1,v2］を選択した場合：

  SNMP コミュニティ名を、1 件以上入力します（ASCII 文字 30 字以内で最大 10 件）。複数入力する場合は、使用頻度が高い順に入力します。

  使用していない SNMP コミュニティ名は削除してください。

  SNMP コミュニティ名は、本機が SNMP 対応機にアクセスするときにパスワードのような働きをします。詳細は、各デバイスの取扱説明書を参照してください。

  デバイスが HTTPS 対応機だけの場合は、SNMP コミュニティ名の入力は不要です。

- ［SNMPv3］を選択した場合：

  ユーザー名、認証用パスワード、暗号化パスワードを 1 セット以上入力します。最大 10 件入力できます。

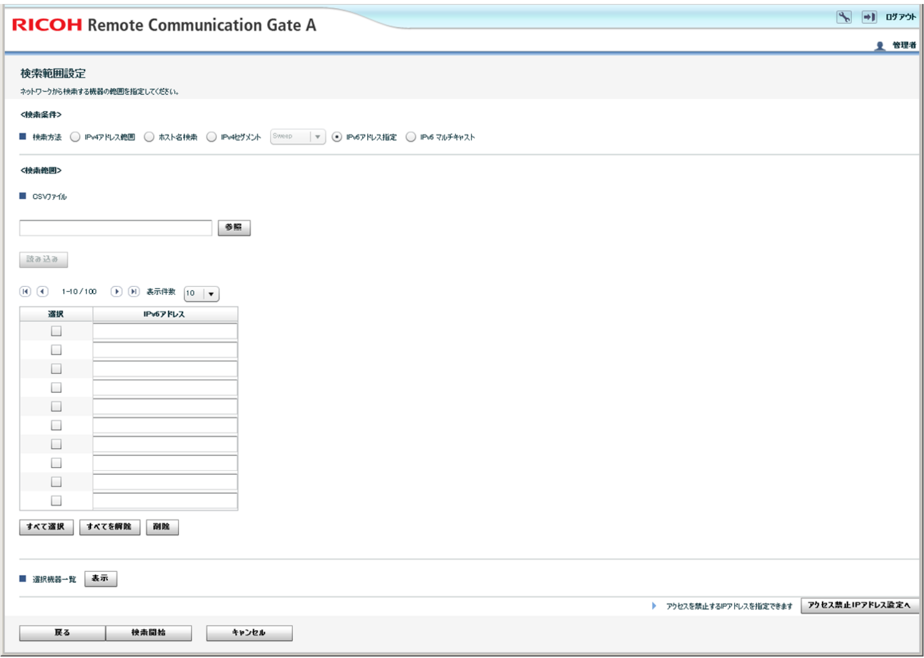
- ［SNMPv3 優先］を選択した場合：

  SNMPv3 と SNMPv1,v2 プロトコルを使用します。最初に SNMPv3 プロトコルを使用して、デバイスを検索します。デバイスが SNMPv3 対応でない場合、SNMPv1,v2 プロトコルを使用して検索します。

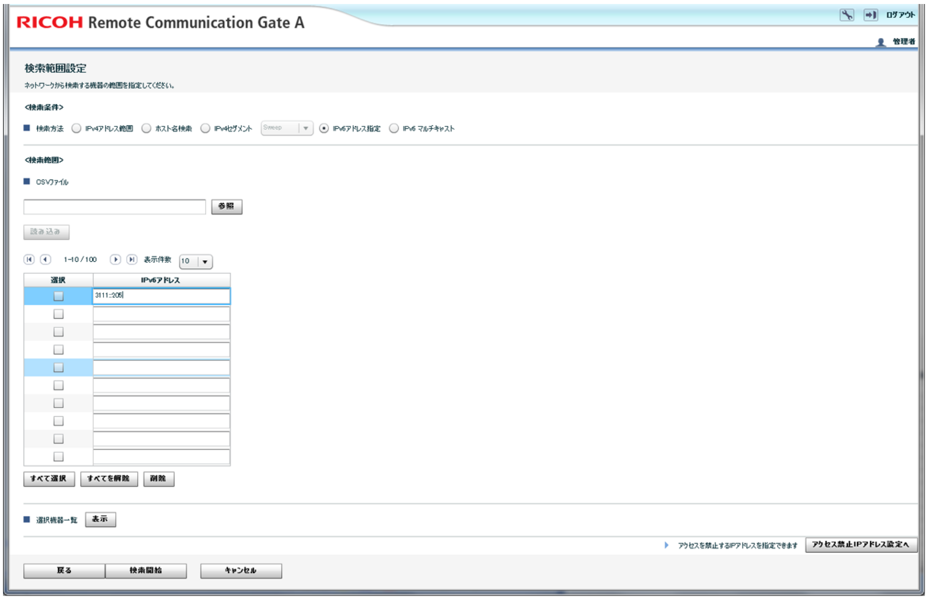
リスト内の項目をすべて選択する場合は、［すべて選択］をクリックします。

項目の選択をすべて解除する場合は、［すべてを解除］をクリックします。

4. 検索方法を［IPv6 アドレス指定］に設定する。



5. 検索範囲を設定する。



- 直接入力する場合：

  IPv6 アドレスを「xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx」形式で入力します。最大 100 件（オプションでメモリーおよびストレージを拡張すると 1,000 件）入力できます。（「x」は 16 進数。連続する「0」は省略できます。）

- CSV ファイルからインポートする場合：

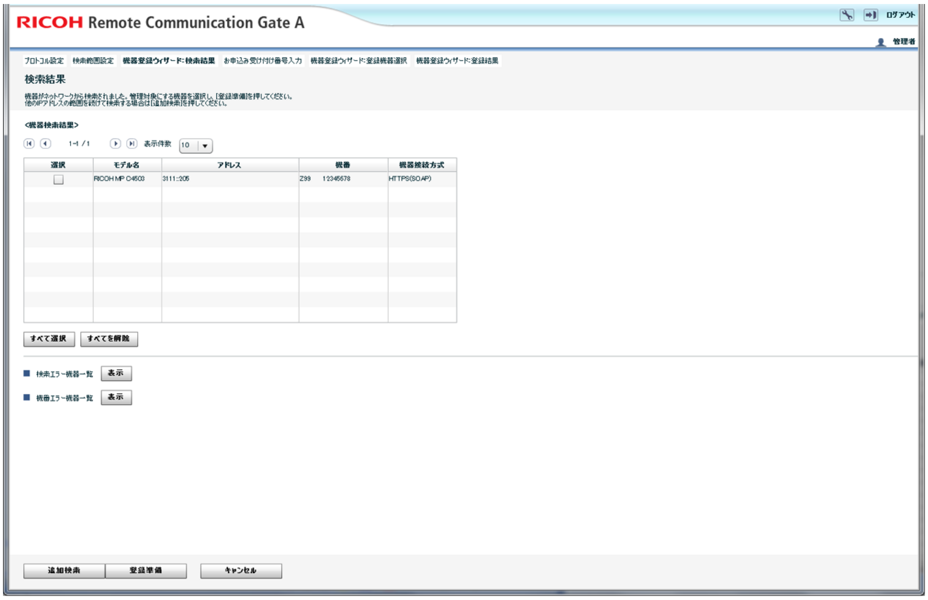
  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた IPv6 は削除されます。

6. ［検索開始］をクリックする。

デバイスの検索が始まります。

7. 検索されたデバイスの中から、登録したいデバイスのチェックボックスを選択し、［登録準備］をクリックする。



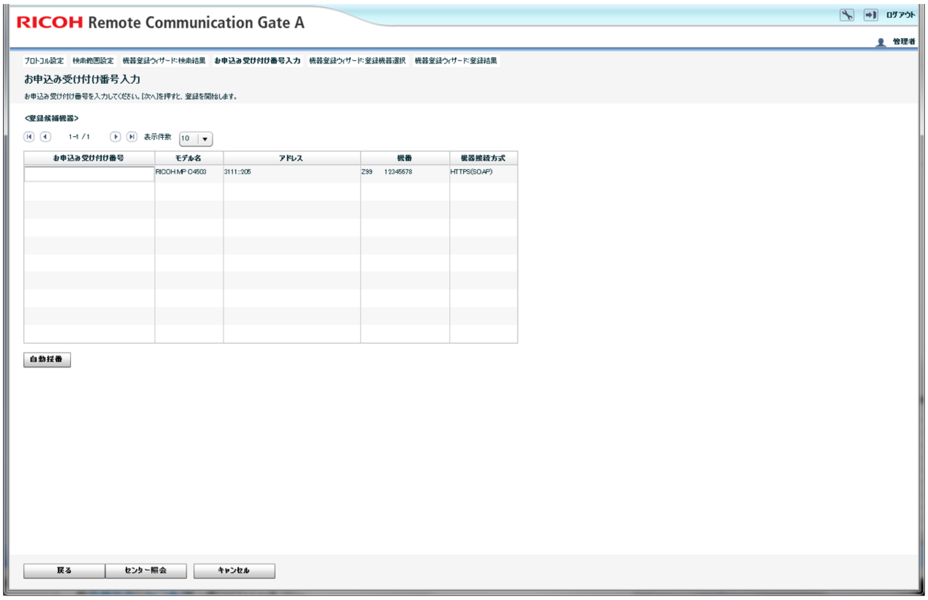
表示ページは、件数表示の左右にあるボタンをクリックして切り替えられます。1 ページに表示する件数は、「表示件数」リストで変更できます。

登録済みデバイスは、［選択］欄がマスク（灰色表示）されます。

- ［すべて選択］：現在のページに表示されていないデバイスを含め、検索されたすべてのデバイスを選択します。
- ［すべてを解除］：現在のページに表示されていないデバイスを含め、項目の選択をすべて解除します。
- ［機番エラー一覧］：本機が機番を識別できないデバイスの IPv6 アドレス、MAC アドレス、モデル名の一覧を表示します。

8. 各デバイスの「お申込み受け付け番号」を入力し、［センター照会］をクリックする。

「お申込み受け付け番号」を自動採番する場合は、［自動採番］をクリックします。



9. **RS センターシステムに登録したいデバイスのチェックボックスを選択し、［登録］をクリックする。**

   各デバイスの機番をクリックすると、照会されたデバイスの詳細情報を確認できます。同一モデルを複数台ご利用の場合は、各デバイスの設置場所を確認してください。

   RS センターシステムへの照会に失敗した場合は、「照会結果」欄に「NG」と表示されます。デバイスの機番をクリックして、詳細画面の「照会結果」欄に表示されている対処方法を確認してください。

10. **登録結果を確認し、［終了］をクリックする。**

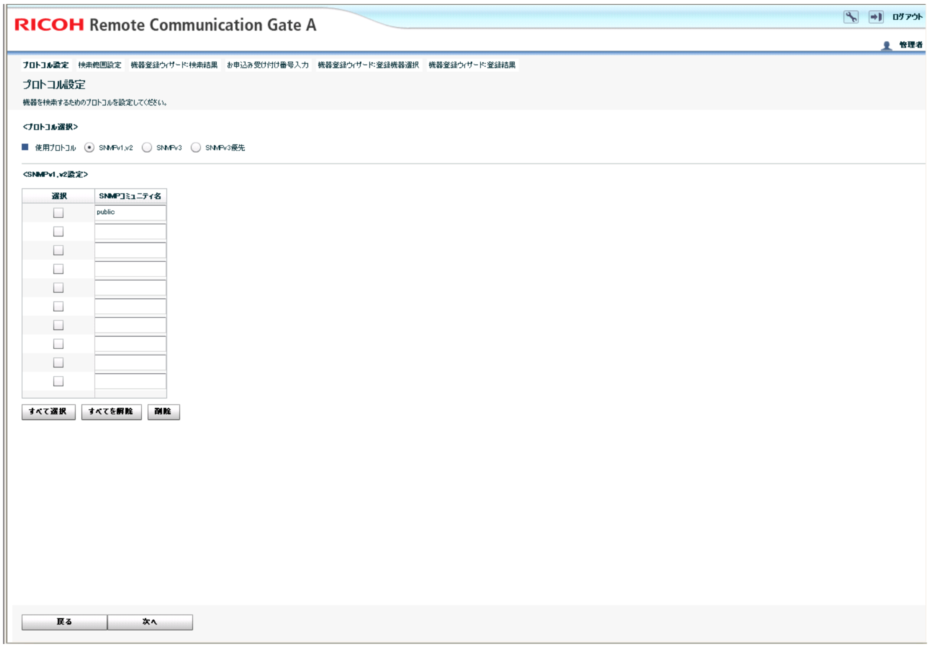
    「導入設定」画面に戻ります。

IPv6 マルチキャストアドレスでデバイスを検索する場合

登録するデバイスの検索範囲を、IPv6 マルチキャストアドレス「FF02::1」で指定する方法を説明します。

1. **RC Gate モニターが起動していない場合は起動し、［管理者］でログインする。**
2. **［機器登録ウィザード］をクリックする。**

3. 検索に使用する SNMP プロトコルを選択し、［次へ］をクリックする。



- ［SNMPv1,v2］を選択した場合：

  SNMP コミュニティ名を、1 件以上入力します（ASCII 文字 30 字以内で最大 10 件）。複数入力する場合は、使用頻度が高い順に入力します。

  使用していない SNMP コミュニティ名は削除してください。

  SNMP コミュニティ名は、本機が SNMP 対応機にアクセスするときにパスワードのような働きをします。詳細は、各デバイスの取扱説明書を参照してください。

  デバイスが HTTPS 対応機だけの場合は、SNMP コミュニティ名の入力は不要です。

- ［SNMPv3］を選択した場合：

  ユーザー名、認証用パスワード、暗号化パスワードを 1 セット以上入力します。最大 10 件入力できます。

- ［SNMPv3 優先］を選択した場合：

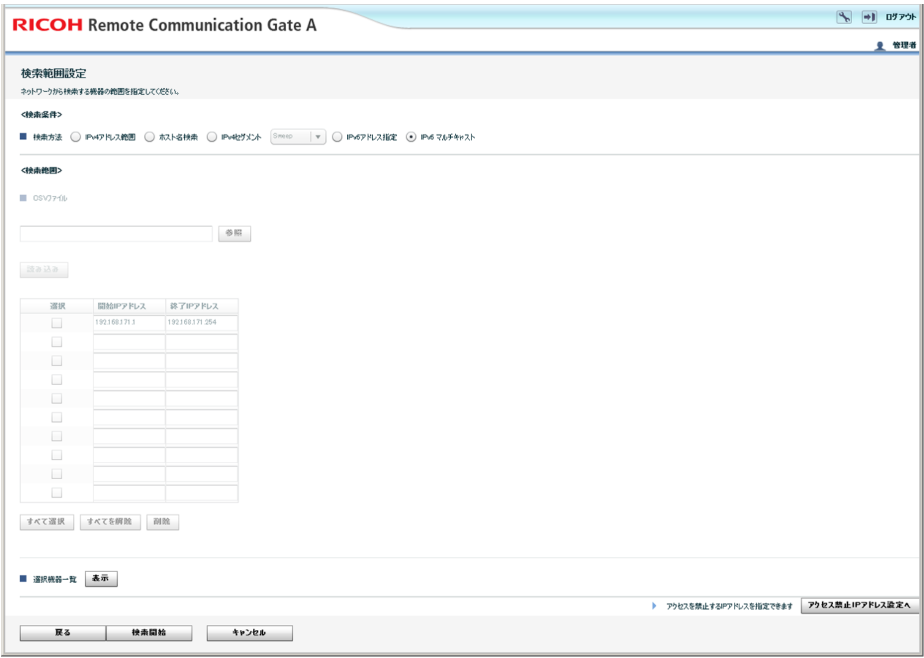
  SNMPv3 と SNMPv1,v2 プロトコルを使用します。最初に SNMPv3 プロトコルを使用して、デバイスを検索します。デバイスが SNMPv3 対応でない場合、SNMPv1,v2 プロトコルを使用して検索します。

リスト内の項目をすべて選択する場合は、［すべて選択］をクリックします。

項目の選択をすべて解除する場合は、［すべてを解除］をクリックします。

2

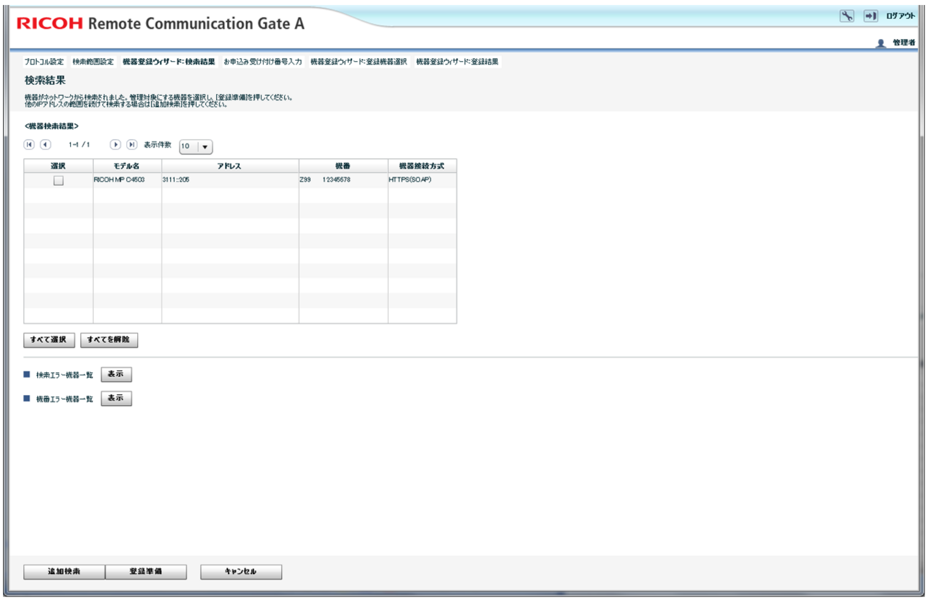
4. 検索方法を［IPv6 マルチキャスト］に設定する。



5. ［検索開始］をクリックする。

デバイスの検索が始まります。

6. 検索されたデバイスの中から、登録したいデバイスのチェックボックスを選択し、［登録準備］をクリックする。



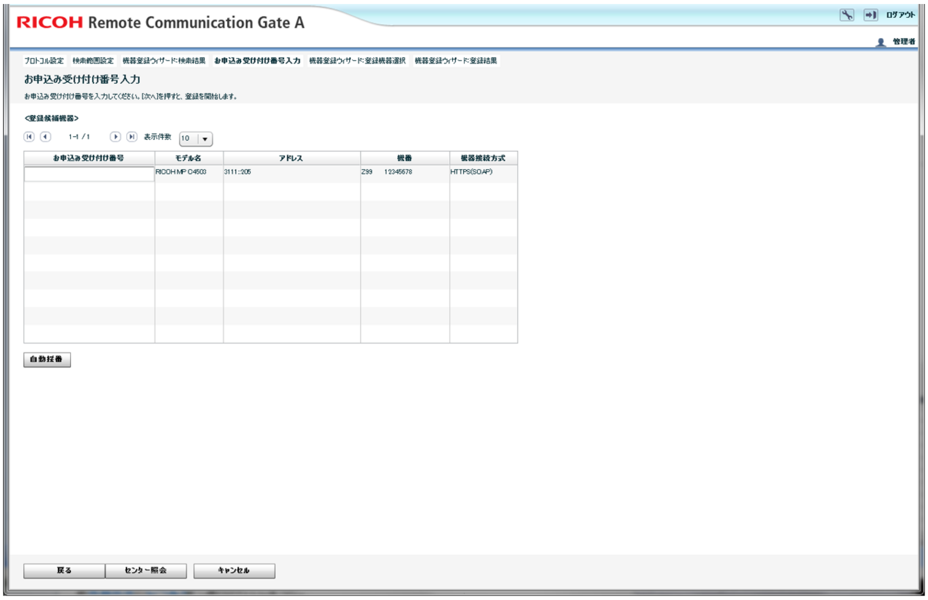
表示ページは、件数表示の左右にあるボタンをクリックして切り替えられます。1ページに表示する件数は、「表示件数」リストで変更できます。

登録済みデバイスは、[選択] 欄がマスク（灰色表示）されます。

- [すべて選択]：現在のページに表示されていないデバイスを含め、検索されたすべてのデバイスを選択します。
- [すべてを解除]：現在のページに表示されていないデバイスを含め、項目の選択をすべて解除します。
- [機番エラー一覧]：本機が機番を識別できないデバイスの IPv6 アドレス、MAC アドレス、モデル名の一覧を表示します。

7. 各デバイスの「お申込み受け付け番号」を入力し、[センター照会] をクリックする。

「お申込み受け付け番号」を自動採番する場合は、[自動採番] をクリックします。



8. RS センターシステムに登録したいデバイスのチェックボックスを選択し、[登録] をクリックする。

機番をクリックすると、照会されたデバイスの詳細情報を確認できます。同一モデルを複数台ご利用の場合は、各デバイスの設置場所を確認してください。

RS センターシステムへの照会に失敗した場合は、「照会結果」欄に「NG」と表示されます。デバイスの機番をクリックして、詳細画面の「照会結果」欄に表示されている対処方法を確認してください。

9. 登録結果を確認し、[終了] をクリックする。

「導入設定」画面に戻ります。

CSV ファイルを作成する

CSV ファイルをインポートするために、あらかじめ CSV ファイルを作成しておきます。

IPv4 アドレスで範囲を指定する場合：

開始 IPv4 アドレスと終了 IPv4 アドレスをカンマ（,）で区切って入力してください。各検索範囲は、異なる行に入力してください。最大 256 行入力できます。

CSV ファイルの入力例

```
192.168.0.1,192.168.0.2
192.168.0.3,192.168.0.4
192.168.0.5,192.168.0.6
192.168.0.7,192.168.0.8
```

BSE019S

ネットワークのセグメントで範囲を指定する場合：

各ネットワークのセグメント情報をカンマ（,）で区切って入力してください。各検索範囲にサブネット IP アドレスとサブネットマスクを入力してください。最大 256 行入力できます。

CSV ファイルの入力例

```
192.168.1.0,255.255.255.0
192.168.2.0,255.255.255.0
192.168.3.0,255.255.255.0
192.168.4.0,255.255.255.0
```

BSE020S

ホスト名で範囲を指定する場合：

各行にホスト名を入力してください。最大 100 行入力できます。

CSV ファイルの入力例

```
host0
host1
host2
host3
host4
```

BSE017S

IPv6 アドレスを指定する場合：

各行に IPv6 アドレスを入力してください。最大 100 行入力できます。

CSV ファイルの入力例

```
2001:DB8::1:0
2001:DB8::2:0
2001:DB8::3:0
2001:DB8::4:0
```

BSE023S

アクセスを禁止したい IP アドレスを指定する場合：

各行にアクセス禁止対象の IP アドレスとコメントをカンマ（,）で区切って入力してください。最大 256 行入力できます。

CSV ファイルの入力例

```
192.168.0.1,GatewayRouter
192.168.0.2,FileServer
```

BSE018S

3. オートディスカバリー設定ウィザードの操作手順

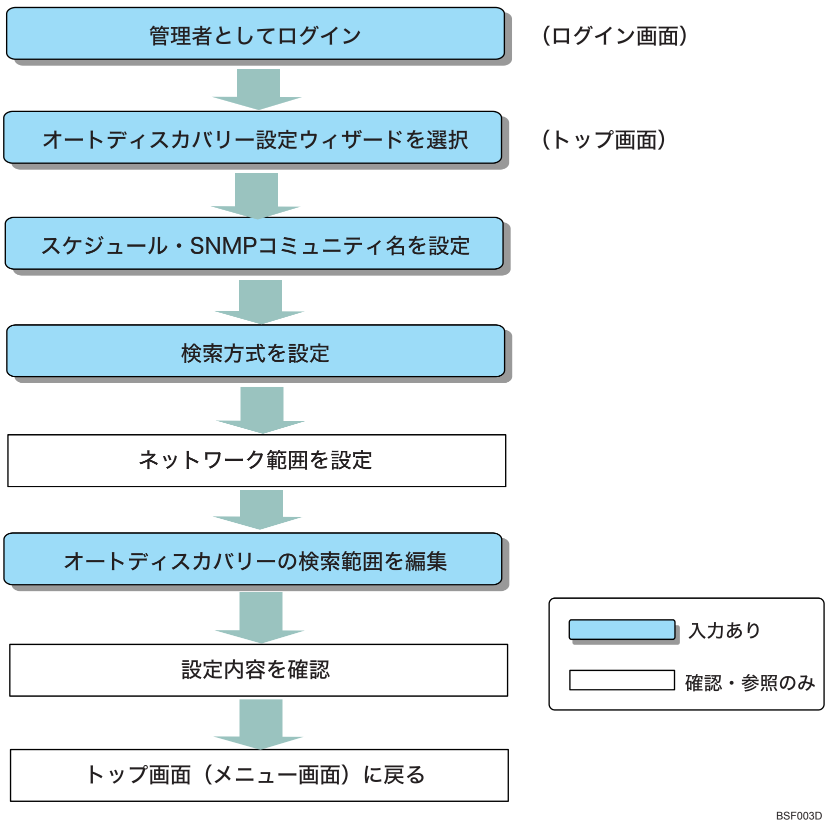
オートディスカバリー機能を有効にすると、RC Gate は指定されたスケジュールでネットワーク上のデバイス情報を収集し、RS センターシステムに送ります。

オートディスカバリーは、「オートディスカバリー設定ウィザード」で設定します。

「オートディスカバリー設定ウィザード」は、管理者でログインしていて、なおかつ「@Remote サービス登録ウィザード」が終了している場合に表示されるメニューです。

オートディスカバリー設定ウィザードの流れ

ここでは、オートディスカバリー機能を設定する流れについて説明します。



オートディスカバリー設定ウィザードの操作手順

ここでは、オートディスカバリー機能を使用して、デバイスを検出する方法を説明します。

以下の 5 つの方法で、ネットワーク上のデバイスを検出できます。

- IP アドレスの範囲を指定して検索する。
- ホスト名を指定して検索する。
- ネットワークのセグメントを指定して検索する。
- IPv6 アドレスを指定して検索する。
- IPv6 アドレスをマルチキャスト検索する。

3

重要

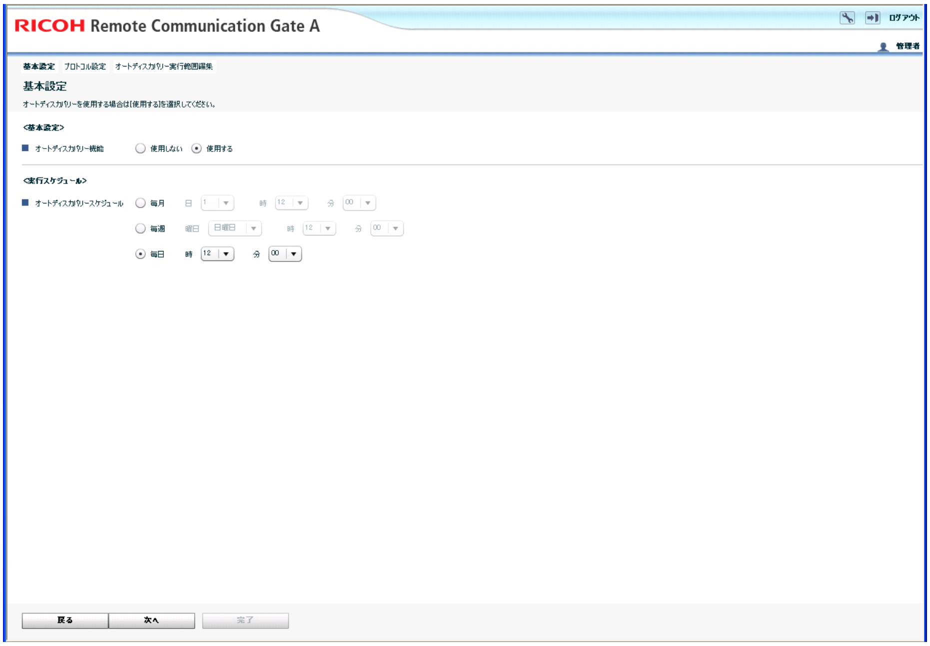
- パソコンに保存された CSV ファイルからもオートディスカバリーの実行範囲をインポートできます。詳細は、P.79「CSV ファイルを作成する」を参照してください。

オートディスカバリーの実行範囲を IPv4 アドレスで指定する場合

オートディスカバリーの実行範囲を、デバイスの IPv4 アドレスで指定する方法を説明します。

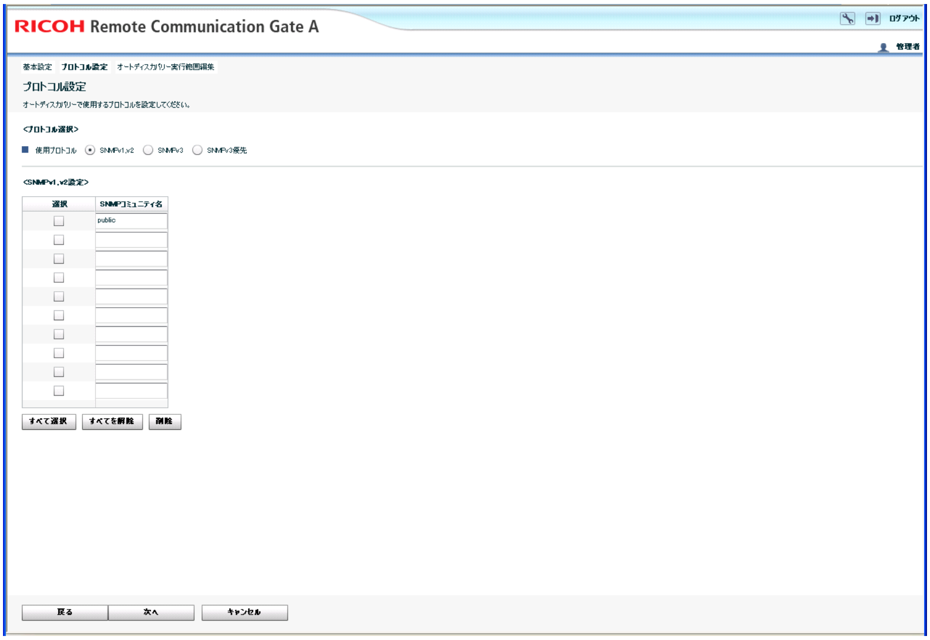
1. **RC Gate モニターが起動していない場合は起動し、［管理者］でログインする。**
2. **［オートディスカバリー設定ウィザード］をクリックする。**

3.「オートディスカバリー機能」を［使用する］に設定する。



4.「<実行スケジュール>」の各項目を設定し、［次へ］をクリックする。

5. 検索に使用する SNMP プロトコルを選択し、［次へ］をクリックする。



- ［SNMPv1,v2］を選択した場合：

SNMP コミュニティ名を、1 件以上入力します（ASCII 文字 30 字以内で最大 10 件）。複数入力する場合は、使用頻度が高い順に入力します。

使用していない SNMP コミュニティ名は削除してください。

SNMP コミュニティ名は、本機が SNMP 対応機にアクセスするときにパスワードのような働きをします。詳細は、各デバイスの取扱説明書を参照してください。

デバイスが HTTPS 対応機だけの場合は、SNMP コミュニティ名の入力は不要です。

- ［SNMPv3］を選択した場合：

  ユーザー名、認証用パスワード、暗号化パスワードを 1 セット以上入力します。最大 10 件入力できます。

- ［SNMPv3 優先］を選択した場合：

  SNMPv3 と SNMPv1,v2 プロトコルを使用します。最初に SNMPv3 プロトコルを使用して、デバイスを検索します。デバイスが SNMPv3 対応でない場合、SNMPv1,v2 プロトコルを使用して検索します。

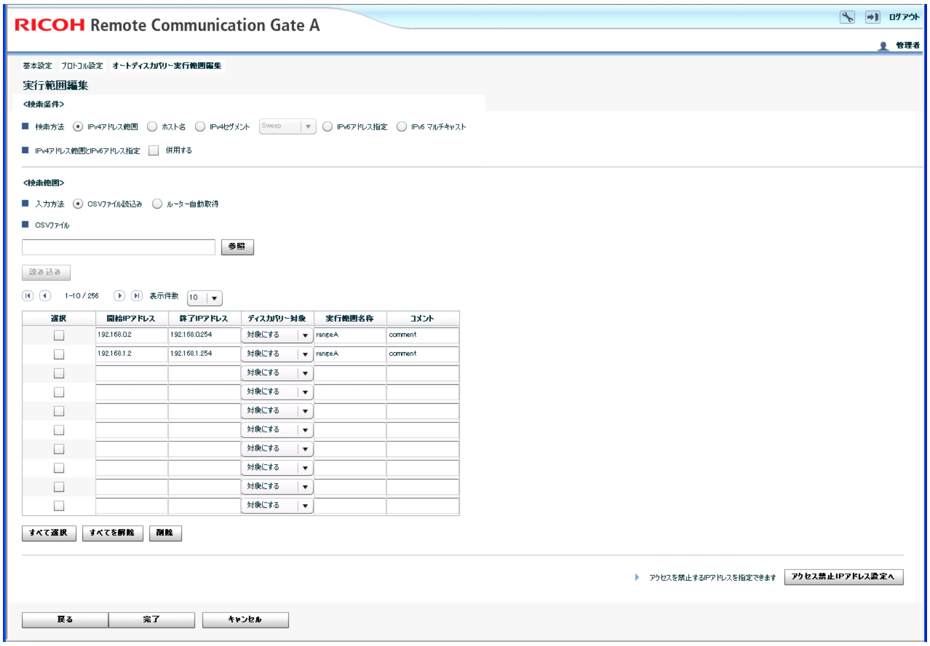
リスト内の項目をすべて選択する場合は、［すべて選択］をクリックします。

項目の選択をすべて解除する場合は、［すべてを解除］をクリックします。

6. 検索方法を［IPv4 アドレス範囲］に設定する。

IPv6 アドレス指定と併用して検索する場合は、［IPv4 アドレス範囲と IPv6 アドレス指定］の［併用する］を選択します。

7. 検索範囲を設定する。



- 直接入力する場合：

検索開始 IPv4 アドレスと検索終了 IPv4 アドレスを「x. x. x. x」形式（「x」は 0～255 の範囲内の整数）で入力します。最大 10 件入力できます。

終了 IPv4 アドレスは、開始 IPv4 アドレスより大きな値を入力します。

検索終了 IPv4 アドレスに「0.0.0.0」を設定した行は検索されません。

検索開始 IPv4 アドレスに「0.0.0.0」を設定して、検索終了 IPv4 アドレスに「0.0.0.0」以外を設定した場合は検索エラーになります。

- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた検索範囲は削除されます。

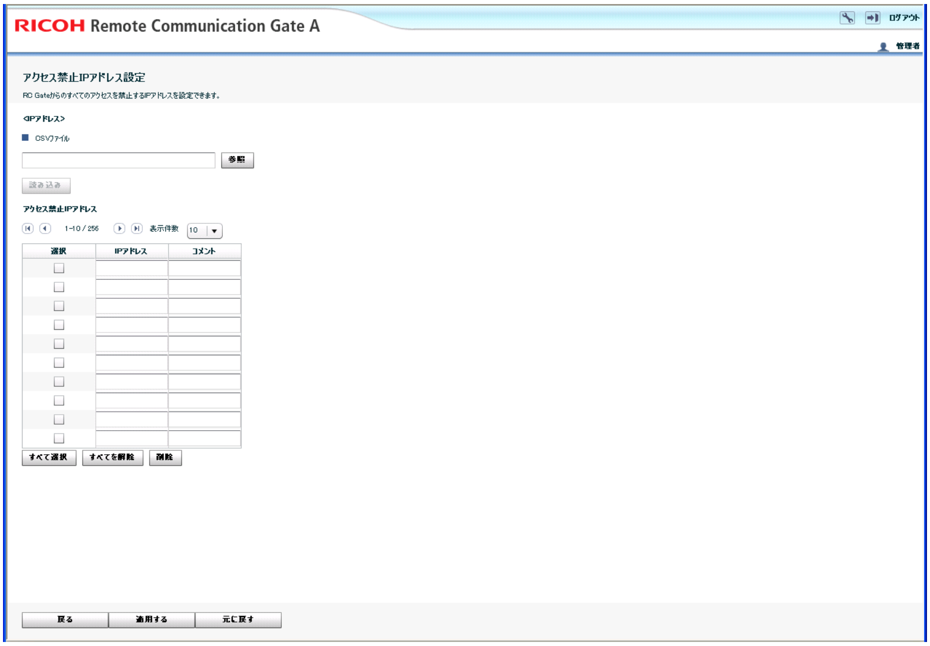
- ルーターで検索する場合：

  ［ルーター自動取得］を選択します。検索ホップ数（0～10）を指定し、［取得開始］をクリックします。

表示ページは、件数表示の左右にあるボタンをクリックして切り替えられます。1 ページに表示する件数は、「表示件数」リストで変更できます。

8. ［アクセス禁止 IP アドレス設定へ］をクリックし、RC Gate からアクセスを禁止するデバイスの IPv4 アドレスを設定する。

アクセスを禁止する IPv4 アドレスを指定しない場合は、手順 10 に進んでください。



- 直接入力する場合：

IPv4 アドレスを「x. x. x. x」形式（「x」は 0〜255 の範囲内の整数）で入力します。最大 256 件入力できます。

- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた IPv4 アドレスは削除されます。

9. アクセスを禁止したい IPv4 アドレスのチェックボックスを選択し、［OK］をクリックする。

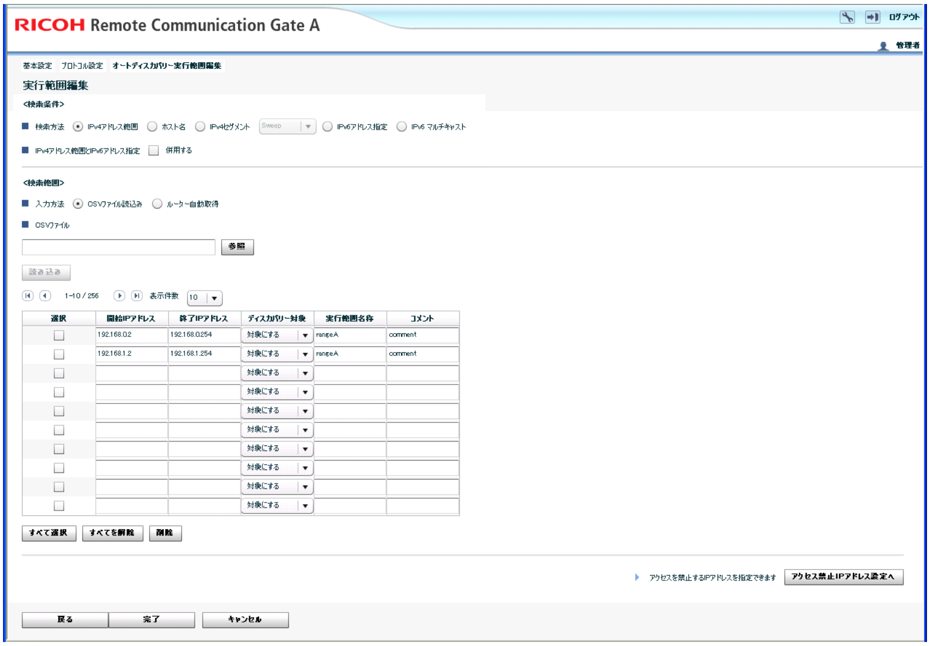
「検索範囲設定」画面に戻ります。

10. 実行範囲を編集する。

実行範囲を削除する場合は、削除したい範囲のチェックボックスを選択し、［削除］をクリックします。

11. 検索されたデバイスに対して、オートディスカバリーの対象にするかしないかを「ディスカバリー対象」で選択する。

必要に応じて、設定した検索範囲の名称を「実行範囲名称」欄に 61 字（ASCII 文字）以内で入力します。

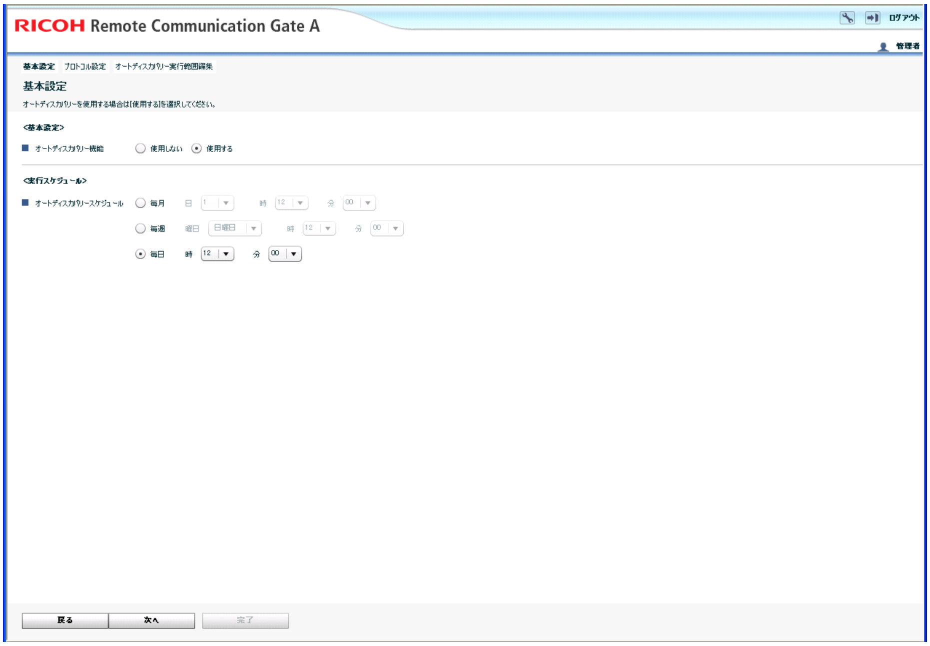


12. ［完了］をクリックする。

オートディスカバリーの実行範囲をホスト名で指定する場合

オートディスカバリーの実行範囲を、ホスト名で指定する方法を説明します。

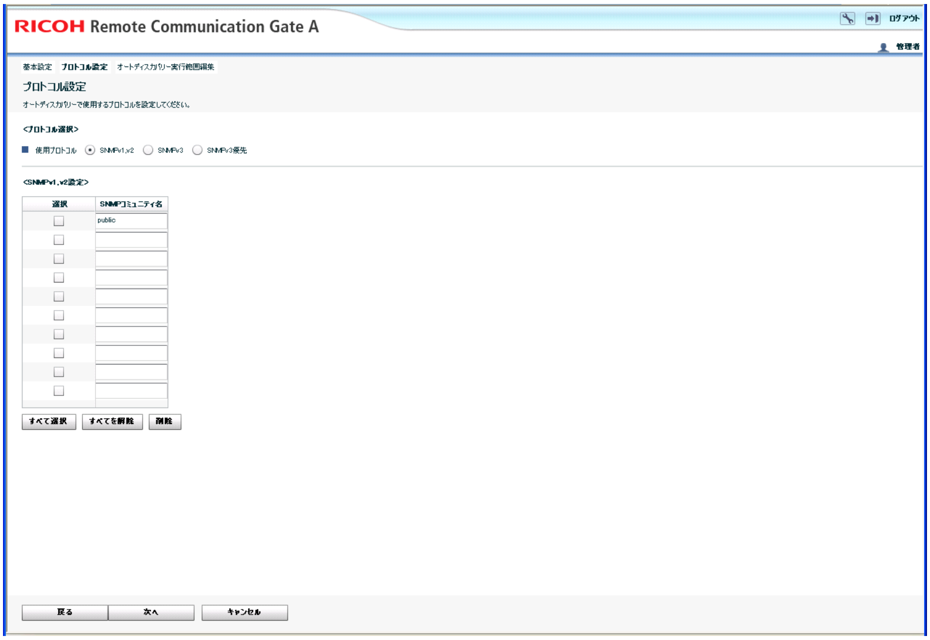
1. RC Gate モニターが起動していない場合は起動し、[管理者] でログインする。
2. [オートディスカバリー設定ウィザード] をクリックする。
3. 「オートディスカバリー機能」を [使用する] に設定する。



4. 「<実行スケジュール>」の各項目を設定し、[次へ] をクリックする。

3

5. **検索に使用する SNMP プロトコルを選択し、［次へ］をクリックする。**



- ［SNMPv1,v2］を選択した場合：

  SNMP コミュニティ名を、1 件以上入力します（ASCII 文字 30 字以内で最大 10 件）。複数入力する場合は、使用頻度が高い順に入力します。

  使用していない SNMP コミュニティ名は削除してください。

  SNMP コミュニティ名は、本機が SNMP 対応機にアクセスするときにパスワードのような働きをします。詳細は、各デバイスの取扱説明書を参照してください。

  デバイスが HTTPS 対応機だけの場合は、SNMP コミュニティ名の入力は不要です。

- ［SNMPv3］を選択した場合：

  ユーザー名、認証用パスワード、暗号化パスワードを 1 セット以上入力します。最大 10 件入力できます。

- ［SNMPv3 優先］を選択した場合：

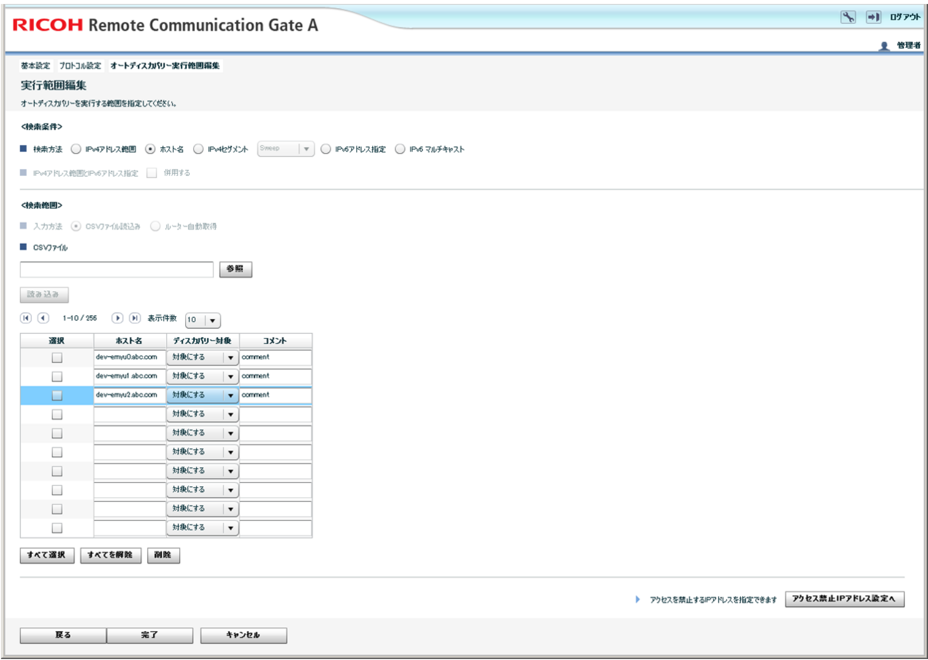
  SNMPv3 と SNMPv1,v2 プロトコルを使用します。最初に SNMPv3 プロトコルを使用して、デバイスを検索します。デバイスが SNMPv3 対応でない場合、SNMPv1,v2 プロトコルを使用して検索します。

リスト内の項目をすべて選択する場合は、［すべて選択］をクリックします。

項目の選択をすべて解除する場合は、［すべてを解除］をクリックします。

6. **検索方法を［ホスト名］に設定する。**

7. 検索範囲を設定する。



- 直接入力する場合：

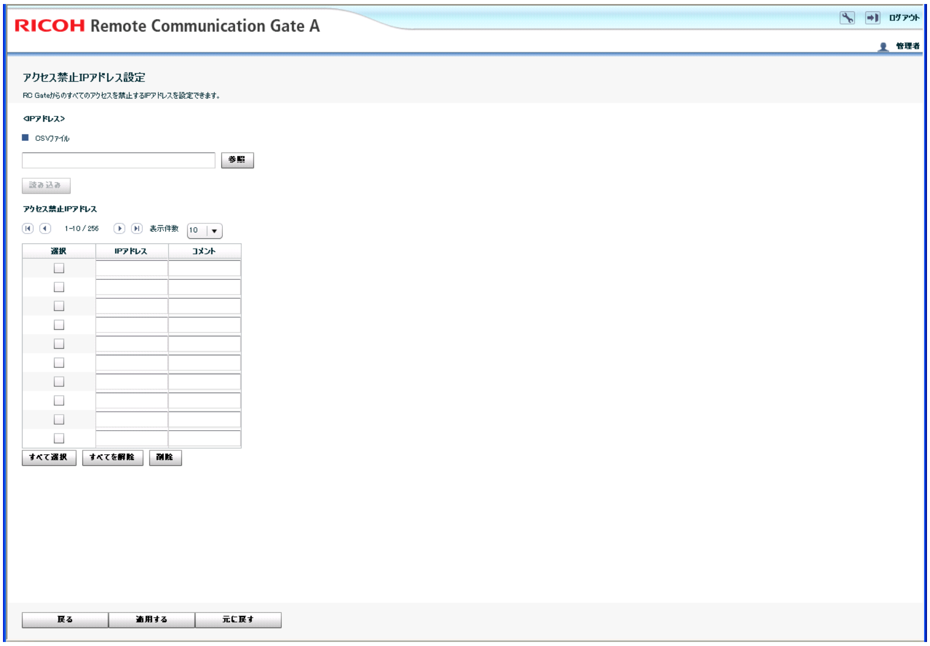
  ホスト名を入力します。最大 100 件（オプションでメモリーおよびストレージを拡張すると 1,000 件）入力できます。

表示ページは、件数表示の左右にあるボタンをクリックして切り替えられます。1 ページに表示する件数は、「表示件数」リストで変更できます。

8. ［アクセス禁止 IP アドレス設定へ］をクリックし、RC Gate からアクセスを禁止するデバイスの IPv4 アドレスを設定する。

アクセスを禁止する IPv4 アドレスを指定しない場合は、手順 10 に進んでください。

3



- 直接入力する場合：

  IPv4 アドレスを「x. x. x. x」形式（「x」は 0〜255 の範囲内の整数）で入力します。最大 256 件入力できます。

- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた IPv4 アドレスは削除されます。

9. アクセスを禁止したい IP アドレスのチェックボックスを選択し、［OK］をクリックする。

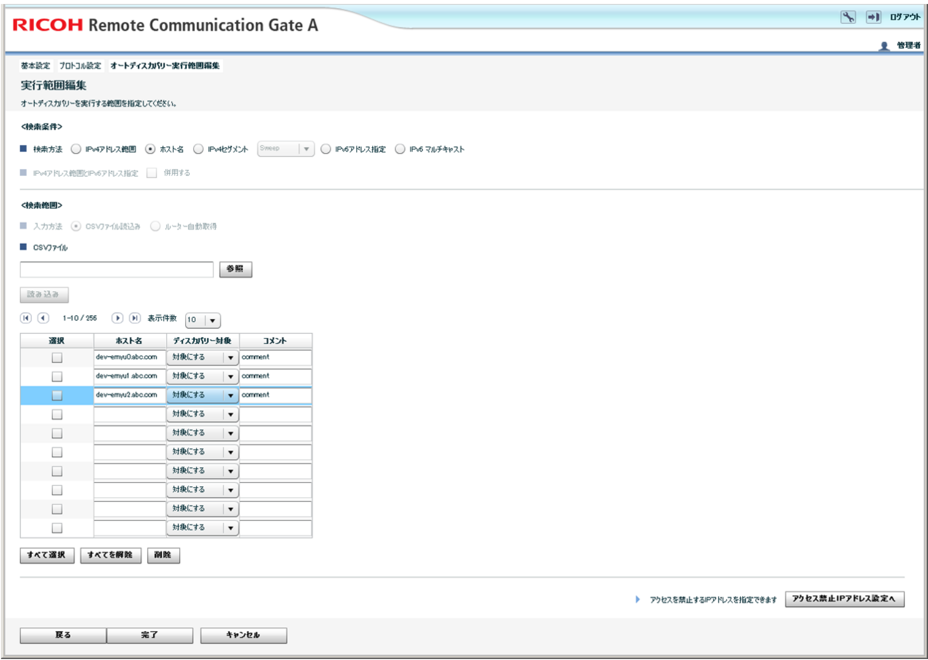
「検索範囲設定」画面に戻ります。

10. 実行範囲を編集する。

実行範囲を削除する場合は、削除したい範囲のチェックボックスを選択し、［削除］をクリックします。

11. 検索されたデバイスに対して、オートディスカバリーの対象にするかしないかを「ディスカバリー対象」で選択する。

必要に応じて、設定した検索範囲の名称を「実行範囲名称」欄に 61 字（ASCII 文字）以内で入力します。



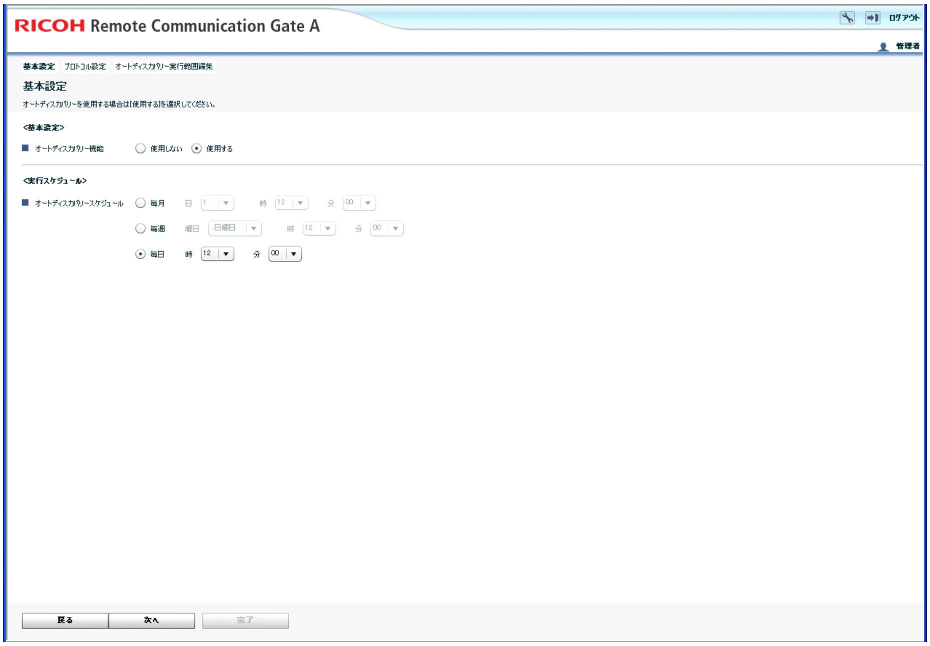
12. ［完了］をクリックする。

オートディスカバリーの実行範囲をセグメントで指定する場合

オートディスカバリーの実行範囲を、ネットワークのセグメントで指定する方法を説明します。

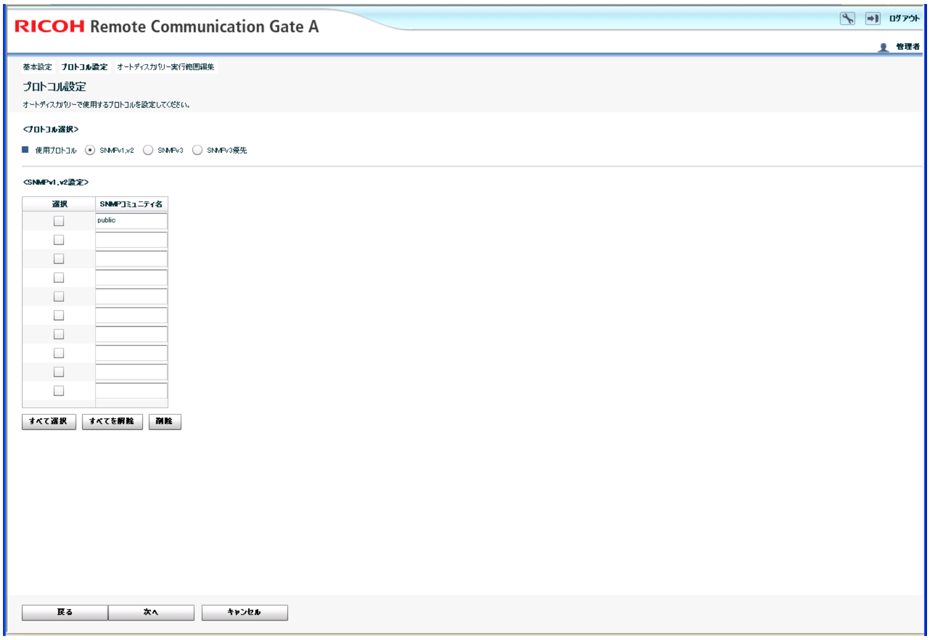
1. RC Gate モニターが起動していない場合は起動し、［管理者］でログインする。
2. ［オートディスカバリー設定ウィザード］をクリックする。

3.「オートディスカバリー機能」を［使用する］に設定する。



4.「<実行スケジュール>」の各項目を設定し、［次へ］をクリックする。

5. 検索に使用する SNMP プロトコルを選択し、［次へ］をクリックする。



- ［SNMPv1,v2］を選択した場合：

SNMP コミュニティ名を、1 件以上入力します（ASCII 文字 30 字以内で最大 10 件）。複数入力する場合は、使用頻度が高い順に入力します。

使用していない SNMP コミュニティ名は削除してください。

SNMP コミュニティ名は、本機が SNMP 対応機にアクセスするときにパスワードのような働きをします。詳細は、各デバイスの取扱説明書を参照してください。

デバイスが HTTPS 対応機だけの場合は、SNMP コミュニティ名の入力は不要です。

- ［SNMPv3］を選択した場合：

  ユーザー名、認証用パスワード、暗号化パスワードを 1 セット以上入力します。最大 10 件入力できます。

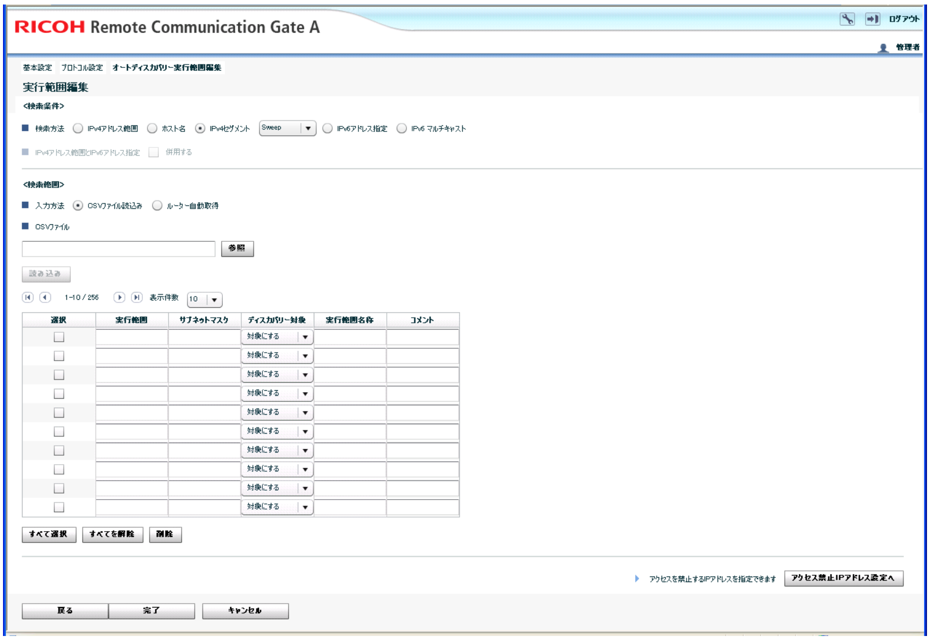
- ［SNMPv3 優先］を選択した場合：

  SNMPv3 と SNMPv1,v2 プロトコルを使用します。最初に SNMPv3 プロトコルを使用して、デバイスを検索します。デバイスが SNMPv3 対応でない場合、SNMPv1,v2 プロトコルを使用して検索します。

リスト内の項目をすべて選択する場合は、［すべて選択］をクリックします。

項目の選択をすべて解除する場合は、［すべてを解除］をクリックします。

6. 検索方法を［IPv4 セグメント］に設定し、検索手段を選択する。



検索手段は、以下から選択します。

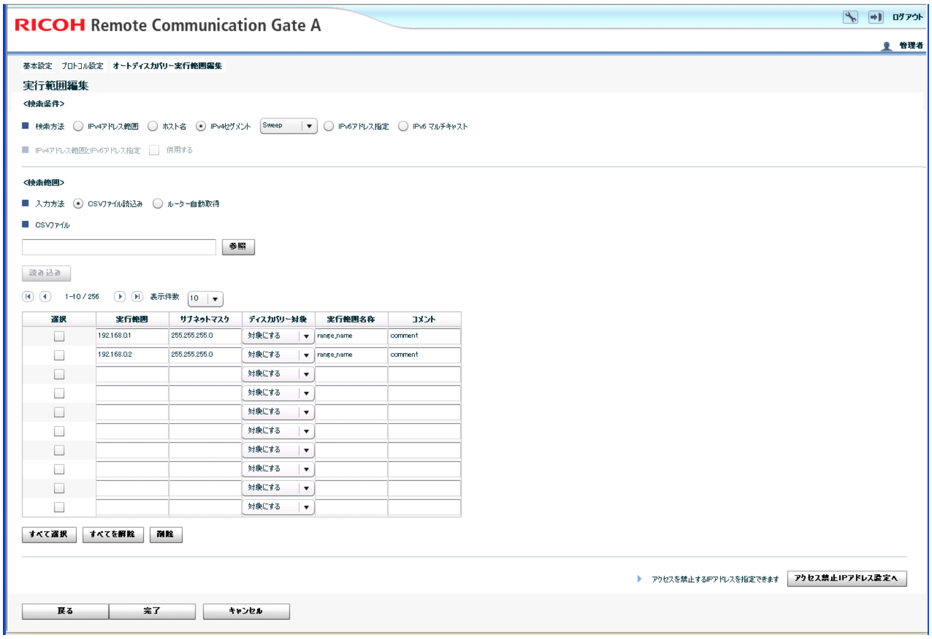
- Sweep によるセグメント検索：

  指定したネットワークセグメントのすべての IPv4 アドレス（ホストアドレス 1～254）に対して、RC Gate が Ping を送信して検索します。

- BroadCast によるセグメント検索：

  指定したネットワークセグメントのブロードキャストアドレスに SNMP をブロードキャストして、応答があった IPv4 アドレスだけを検索します。

7. 検索範囲を設定する。



- 直接入力する場合：

  サブネット IPv4 アドレス、サブネットマスク、検索範囲名を入力します。最大 10 件入力できます。

- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた検索範囲は削除されます。

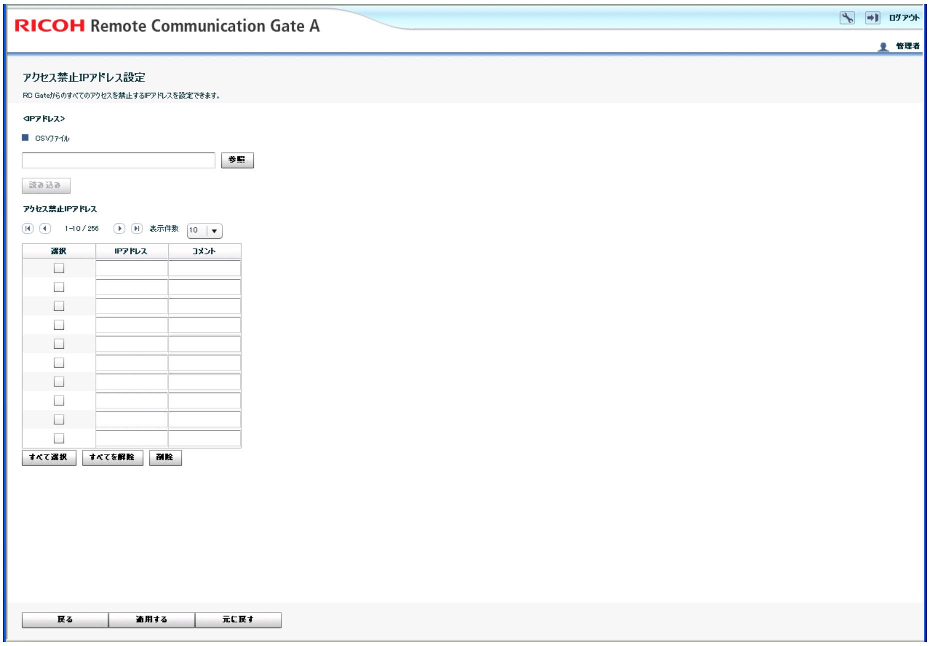
- ルーターで検索する場合：

  ［ルーター自動取得］を選択します。検索ホップ数（0〜10）を指定して［取得開始］をクリックします。

表示ページは、件数表示の左右にあるボタンをクリックして切り替えられます。 1 ページに表示する件数は、「表示件数」リストで変更できます。

8. ［アクセス禁止 IP アドレス設定へ］をクリックし、RC Gate からアクセスを禁止するデバイスの IPv4 アドレスを入力する。

アクセスを禁止する IPv4 アドレスを指定しない場合は、手順 10 に進んでください。



- 直接入力する場合：

  IPv4 アドレスを「x. x. x. x」形式（「x」は 0〜255 の範囲内の整数）で入力します。最大 256 件入力できます。

- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた IPv4 アドレスは削除されます。

9. アクセスを禁止したい IPv4 アドレスのチェックボックスを選択し、［OK］をクリックする。

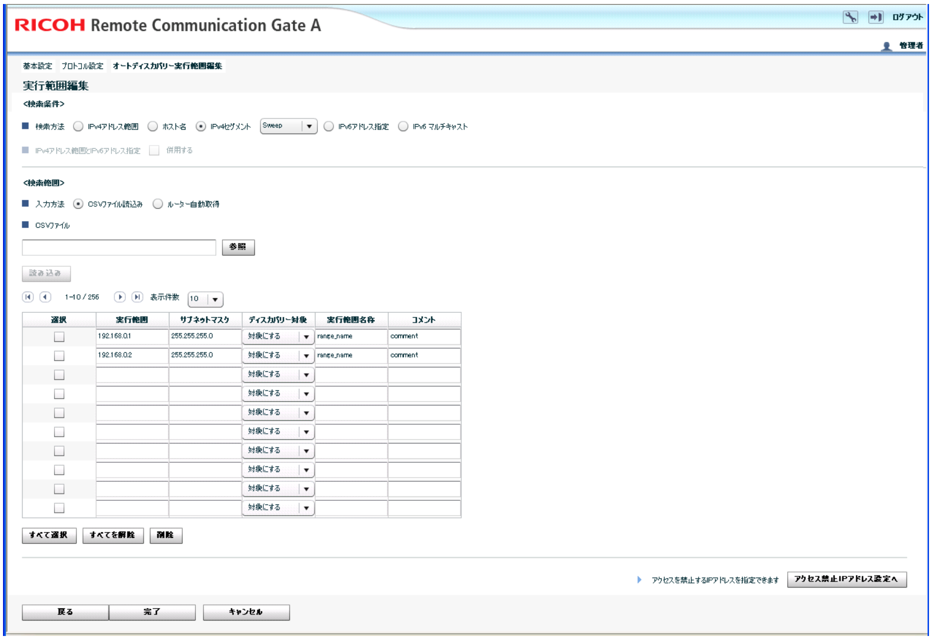
「検索範囲設定」画面に戻ります。

10. 実行範囲を編集する。

実行範囲を削除する場合は、削除したい範囲のチェックボックスを選択し、［削除］をクリックします。

11. 検索されたデバイスに対して、オートディスカバリーの対象にするかしないかを「ディスカバリー対象」で選択する。

必要に応じて、設定した検索範囲の名称を「実行範囲名称」欄に 61 字（ASCII 文字）以内で入力します。



12. [完了] をクリックする。

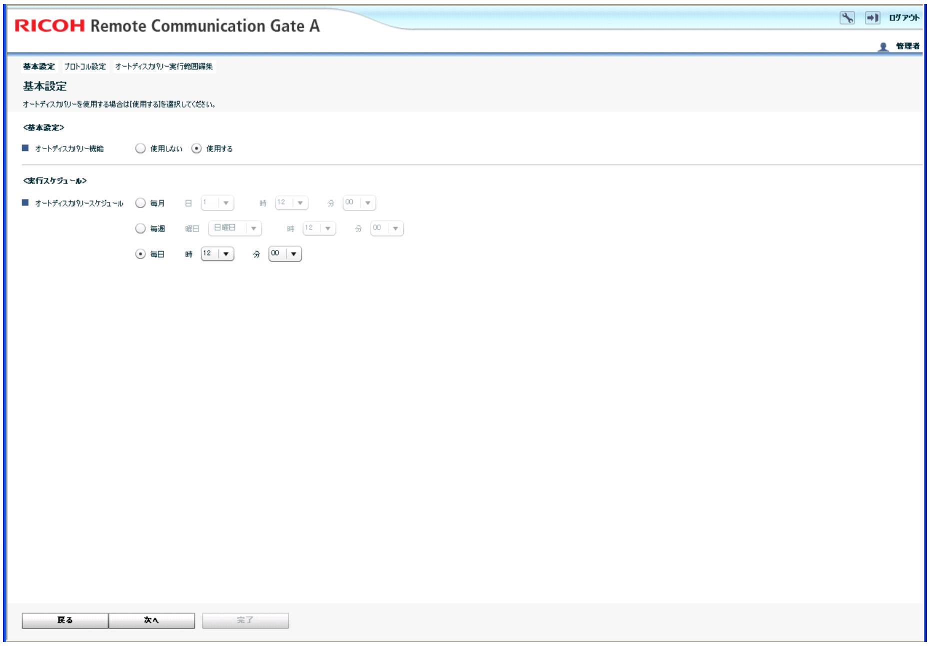
オートディスカバリーの実行範囲を IPv6 アドレスで指定する場合

オートディスカバリーの実行範囲を、IPv6 アドレスで指定する方法を説明します。

1. RC Gate モニターが起動していない場合は起動し、[管理者] でログインする。

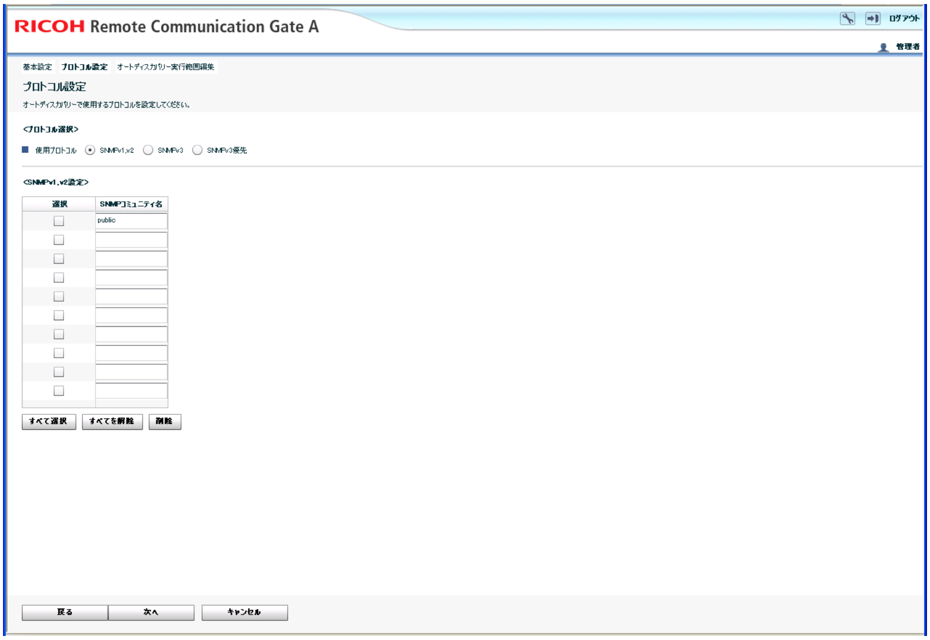
2. [オートディスカバリー設定ウィザード] をクリックする。

3.「オートディスカバリー機能」を［使用する］に設定する。



4.「<実行スケジュール>」の各項目を設定し、［次へ］をクリックする。

5. 検索に使用する SNMP プロトコルを選択し、［次へ］をクリックする。



- ［SNMPv1,v2］を選択した場合：

SNMP コミュニティ名を、1 件以上入力します（ASCII 文字 30 字以内で最大 10 件）。複数入力する場合は、使用頻度が高い順に入力します。

使用していない SNMP コミュニティ名は削除してください。

SNMP コミュニティ名は、本機が SNMP 対応機にアクセスするときにパスワードのような働きをします。詳細は、各デバイスの取扱説明書を参照してください。

デバイスが HTTPS 対応機だけの場合は、SNMP コミュニティ名の入力は不要です。

- ［SNMPv3］を選択した場合：

  ユーザー名、認証用パスワード、暗号化パスワードを 1 セット以上入力します。最大 10 件入力できます。

- ［SNMPv3 優先］を選択した場合：

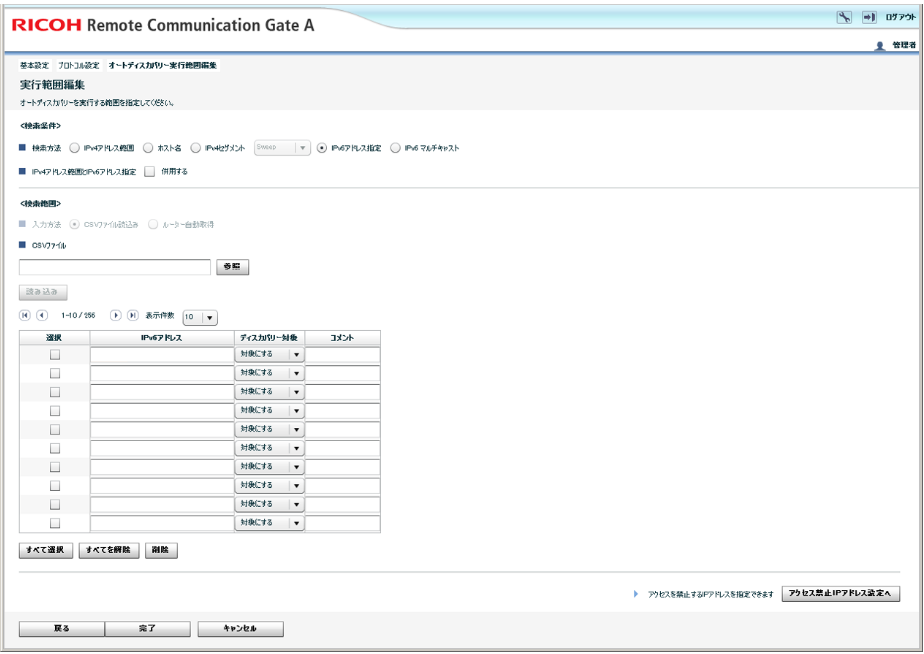
  SNMPv3 と SNMPv1,v2 プロトコルを使用します。最初に SNMPv3 プロトコルを使用して、デバイスを検索します。デバイスが SNMPv3 対応でない場合、SNMPv1,v2 プロトコルを使用して検索します。

リスト内の項目をすべて選択する場合は、［すべて選択］をクリックします。

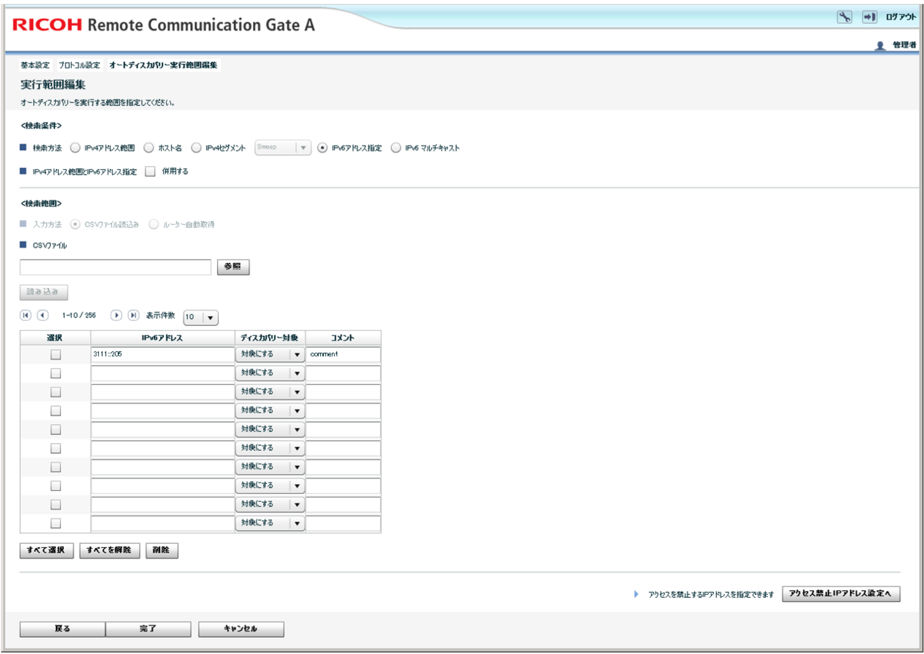
項目の選択をすべて解除する場合は、［すべてを解除］をクリックします。

6. 検索方法を［IPv6 アドレス指定］に設定する。

IPv4 アドレス範囲と併用して検索する場合は、［IPv4 アドレス範囲と IPv6 アドレス指定］の［併用する］を選択します。



7. 検索範囲を設定する。



- 直接入力する場合：

  IPv6 アドレスを「xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx」形式で入力します。(「x」は 16 進数。連続する「0」は省略できます。）最大 100 件（オプションでメモリーおよびストレージを拡張すると 1,000 件）入力できます。

- CSV ファイルからインポートする場合：

  ［参照］をクリックし、CSV ファイルが保存されている場所を指定して［読み込み］をクリックします。

  CSV ファイルから検索範囲をインポートすると、インポート前に入力していた検索範囲は削除されます。

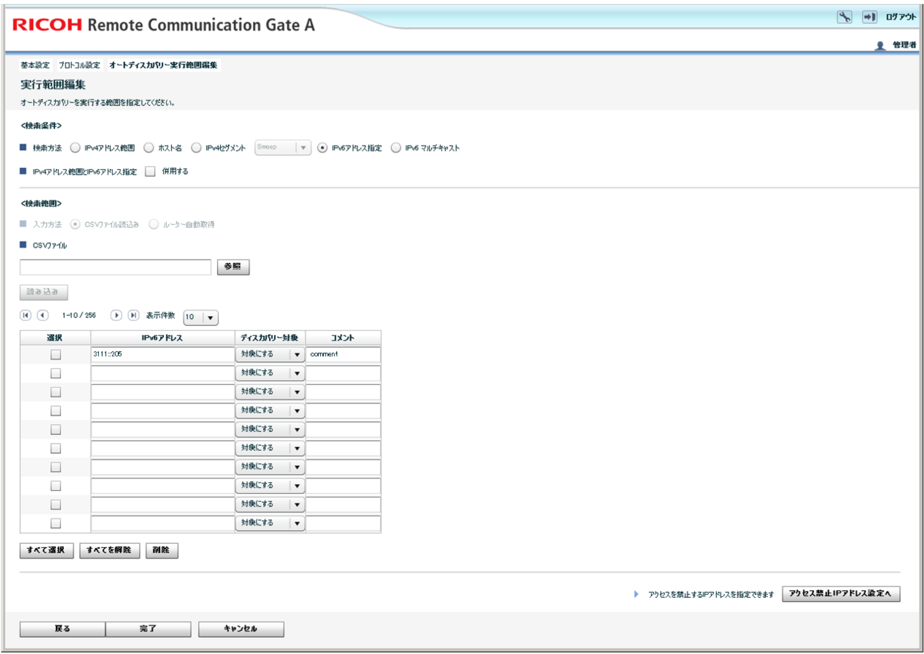
表示ページは、件数表示の左右にあるボタンをクリックして切り替えられます。 1 ページに表示する件数は、「表示件数」リストで変更できます。

8. 実行範囲を編集する。

実行範囲を削除する場合は、削除したい範囲のチェックボックスを選択し、［削除］をクリックします。

9. 検索されたデバイスに対して、オートディスカバリーの対象にするかしないかを「ディスカバリー対象」で選択する。

必要に応じて、設定した検索範囲の名称を「実行範囲名称」欄に 61 字（ASCII 文字）以内で入力します。



10. [完了] をクリックする。

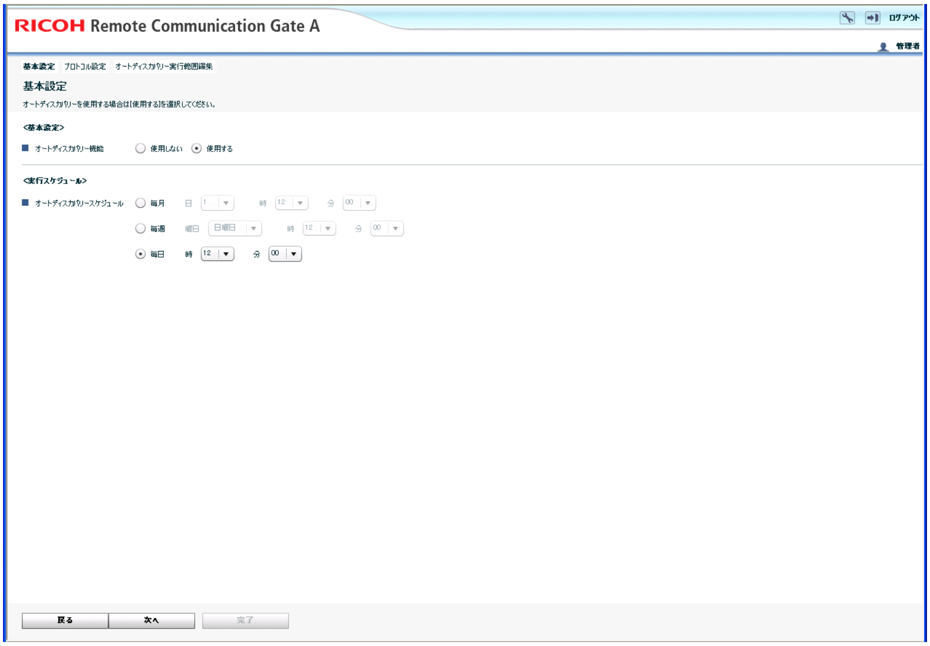
オートディスカバリーの実行範囲を IPv6 マルチキャストアドレスで指定する場合

オートディスカバリーの実行範囲を、IPv6 マルチキャストアドレス「FF02::1」で指定する方法を説明します。

1. RC Gate モニターが起動していない場合は起動し、[管理者] でログインする。

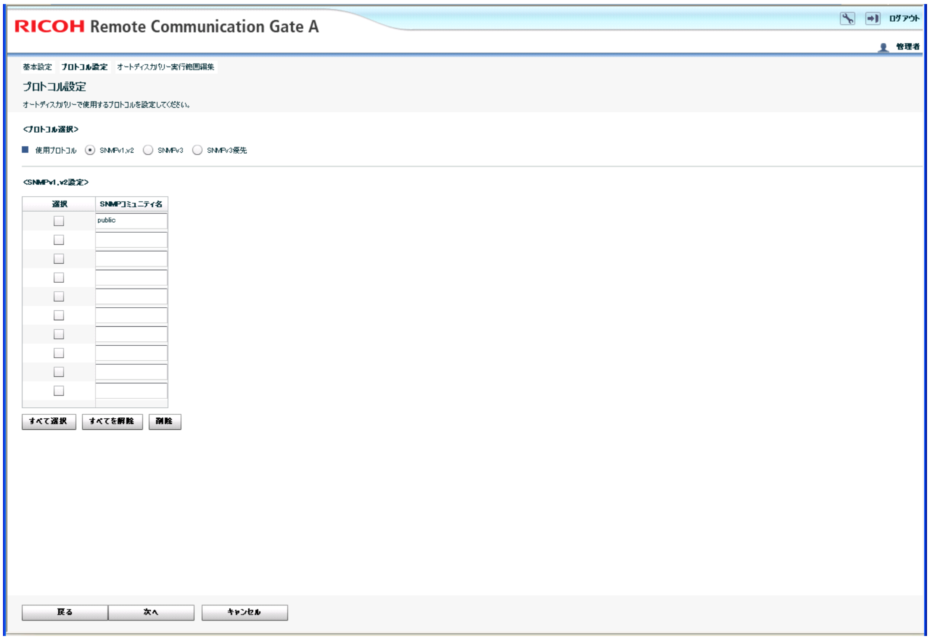
2. [オートディスカバリー設定ウィザード] をクリックする。

3.「オートディスカバリー機能」を［使用する］に設定する。



4.「<実行スケジュール>」の各項目を設定し、［次へ］をクリックする。

5. 検索に使用する SNMP プロトコルを選択し、［次へ］をクリックする。



- ［SNMPv1,v2］を選択した場合：

3

SNMP コミュニティ名を、1 件以上入力します（ASCII 文字 30 字以内で最大 10 件）。複数入力する場合は、使用頻度が高い順に入力します。

使用していない SNMP コミュニティ名は削除してください。

SNMP コミュニティ名は、本機が SNMP 対応機にアクセスするときにパスワードのような働きをします。詳細は、各デバイスの取扱説明書を参照してください。

デバイスが HTTPS 対応機だけの場合は、SNMP コミュニティ名の入力は不要です。

- ［SNMPv3］を選択した場合：

  ユーザー名、認証用パスワード、暗号化パスワードを 1 セット以上入力します。最大 10 件入力できます。

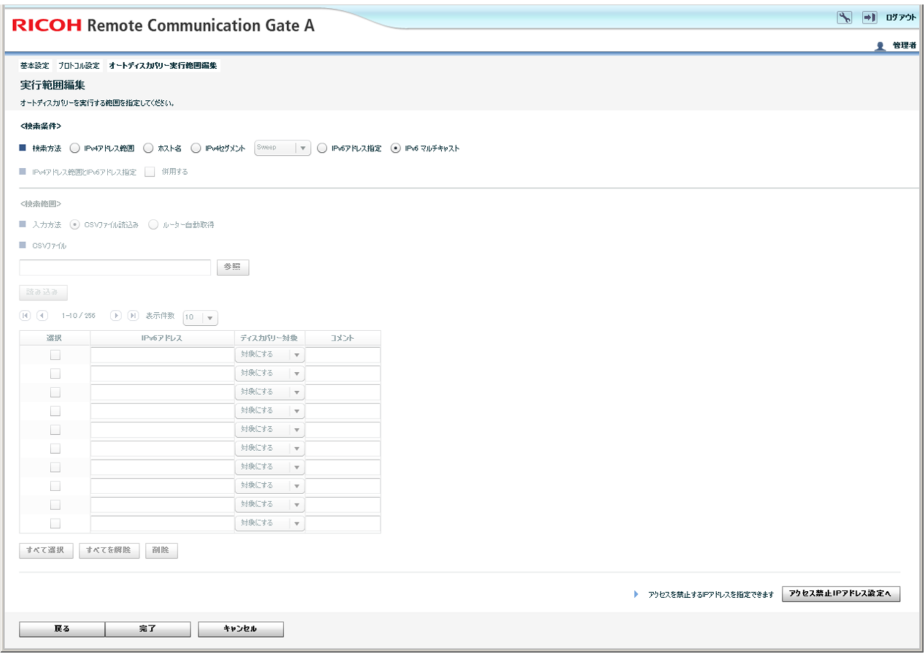
- ［SNMPv3 優先］を選択した場合：

  SNMPv3 と SNMPv1,v2 プロトコルを使用します。最初に SNMPv3 プロトコルを使用して、デバイスを検索します。デバイスが SNMPv3 対応でない場合、SNMPv1,v2 プロトコルを使用して検索します。

リスト内の項目をすべて選択する場合は、［すべて選択］をクリックします。

項目の選択をすべて解除する場合は、［すべてを解除］をクリックします。

6. 検索方法を［IPv6 マルチキャスト］に設定する。



7. ［完了］をクリックする。

CSV ファイルを作成する

CSV ファイルをインポートするために、あらかじめ CSV ファイルを作成しておきます。

IPv4 アドレスで範囲を指定する場合：

各 IPv4 アドレス範囲の情報をカンマ（,）で区切って入力してください。各行には、開始 IPv4 アドレス、終了 IPv4 アドレス、ディスカバリー対象、検索範囲名、コメントを入力してください。最大 256 行入力できます。

CSV ファイルの入力例

```
192.168.0.1,192.168.0.2,Enable,abc,1-63
192.168.0.3,192.168.0.4,Disable,def,64-127
192.168.0.5,192.168.0.6,Enable,ghi,128-191
192.168.0.7,192.168.0.8,Enable,jkl,192-254
```

BSE015S

ネットワークセグメントで範囲を指定する場合：

各ネットワークのセグメント情報をカンマ（,）で区切って入力してください。各検索範囲にサブネット IP アドレス、サブネットマスク、ディスカバリー対象、検索範囲名、コメントを入力してください。最大 256 行入力できます。

CSV ファイルの入力例

```
192.168.1.0,255.255.255.0,Enable,abc,1-63
192.168.2.0,255.255.255.0,Disable,def,64-127
192.168.3.0,255.255.255.0,Enable,ghi,128-191
192.168.4.0,255.255.255.0,Enable,jkl,192-254
```

BSE016S

ホスト名で範囲を指定する場合：

各ホスト名の情報をカンマ（,）で区切って入力してください。各行には、ホスト名、ディスカバリー対象、コメントを入力してください。最大 100 行入力できます。

CSV ファイルの入力例

```
host0,Enable
host1,Disable
host2,Enable
host3,Enable
host4,Disable
```

BSE021S

IPv6 アドレスを指定する場合：

各 IPV6 アドレスの情報をカンマ（,）で区切って入力してください。各行には、IPv6 アドレス、ディスカバリー対象、コメントを入力してください。最大 100 行入力できます。

CSV ファイルの入力例

```
2001:DB8::1:0,Enable
2001:DB8::2:0,Disable
2001:DB8::3:0,Enable
2001:DB8::4:0,Enable
```

BSE022S

アクセスを禁止したい IP アドレスを指定する場合：

各行にアクセス禁止対象の IP アドレスとコメントをカンマ（,）で区切って入力してください。最大 256 行入力できます。

CSV ファイルの入力例

```
192.168.0.1,GatewayRouter
192.168.0.2,FileServer
```

BSE018S

4. 登録内容の詳細を参照・変更する

ここでは、[RC Gate 情報確認/設定]の各画面でできる操作について説明します。

メニューツリーに表示される画面名

ログイン時に[RC Gate 情報確認/設定]を選択した場合に表示されるメニューについて説明します。[管理者]と[一般ユーザー]では、表示されるメニュー・画面が異なります。

管理者



一般ユーザー



RC Gate 設定

画面名	画面概要
基本	本機の基本情報を表示します。
日付・時刻	本機に内蔵された時計を調整します。
ネットワーク	本機のネットワークの設定をします。
プロキシ	HTTP プロキシの設定をします。
メール	管理者に送信するメールの種類を設定します。
アクセス禁止 IP アドレス	本機からのアクセスを禁止するネットワークデバイスの IP アドレスの設定をします。
Ping 接続	ネットワーク上のデバイスを検索するときに、Ping による検索を許可するかしないかを設定します。

オートディスカバリー

画面名	画面概要
基本設定	オートディスカバリーの使用可否、スケジュールなどの基本設定をします。
プロトコル設定	オートディスカバリー検索時のプロトコルの設定をします。

4

画面名	画面概要
オートディスカバリー実行範囲編集	オートディスカバリーを行う IP アドレスやネットワークセグメントの範囲を設定します。

機器管理

画面名	画面概要
機器検索拡張設定	デバイスの拡張検索を有効にするかを設定します。
登録機器一覧	本機が管理しているデバイスの情報を表示します。
機器コール通知履歴	本機が管理しているデバイスからのコールを通知した日付、コール種別、デバイス情報を表示します。
機器共通管理	本機が管理しているデバイスの共通設定を表示します。
機器ファームウェア更新時刻シフト設定	ファームウェア更新の実行時刻を、ネットワークのセグメント単位で設定します。
機器ファームウェア更新	RS センターシステムからの通知が届いた場合、本機が管理しているデバイスのファームウェアを更新します。
機器ファームウェア更新前回履歴	デバイスのファームウェア更新の前回履歴を表示します。

メンテナンス

画面名	画面概要
機能拡張設定	オプションのメモリーおよびストレージが装着されている場合に、1,000 台までデバイスを登録できるように設定します。 いったん［拡張する］に設定すると、［拡張しない］に変更できません。［拡張しない］に戻したい場合は、サービス実施店にご連絡ください。
通信テストコール	RS センターシステムとの通信をテストします。
機器確認依頼コール	RS センターシステムとの通信をテストし、結果を RS センターシステムに通知します。
RC Gate 再起動	本機を再起動します。
RC Gate シャットダウン	本機をシャットダウンします。
サービスコール	障害が発生した場合に、障害内容を表示します。
システム状態	本機のシステム状態を表示します。

4

セキュリティ

画面名	画面概要
ユーザーアカウント設定	RC Gate モニターにアクセスするユーザーアカウントの設定をします。
アクセス許可	カスタマーエンジニアによるログインを制限します。
@Remote サービス機能制限	"@Remote サービス"の機能を制限します。

ユーザー別カウンター

画面名	画面概要
ユーザー別カウンター取得基本設定	ユーザー別カウンターを取得する場合に、デバイスから情報取得するために必要な設定をします。
ユーザー別カウンター取得対象機器一覧	ユーザー別カウンターを取得する場合に、情報取得対象のデバイスを一覧表示します。
ユーザー別カウンター取得テスト	ユーザー別カウンターを取得する場合に、デバイスから情報取得できるか確認を行います。

ログ

画面名	画面概要
セキュリティログ	RC Gate モニターにアクセスしたユーザーのログを表示します。

画面の詳細

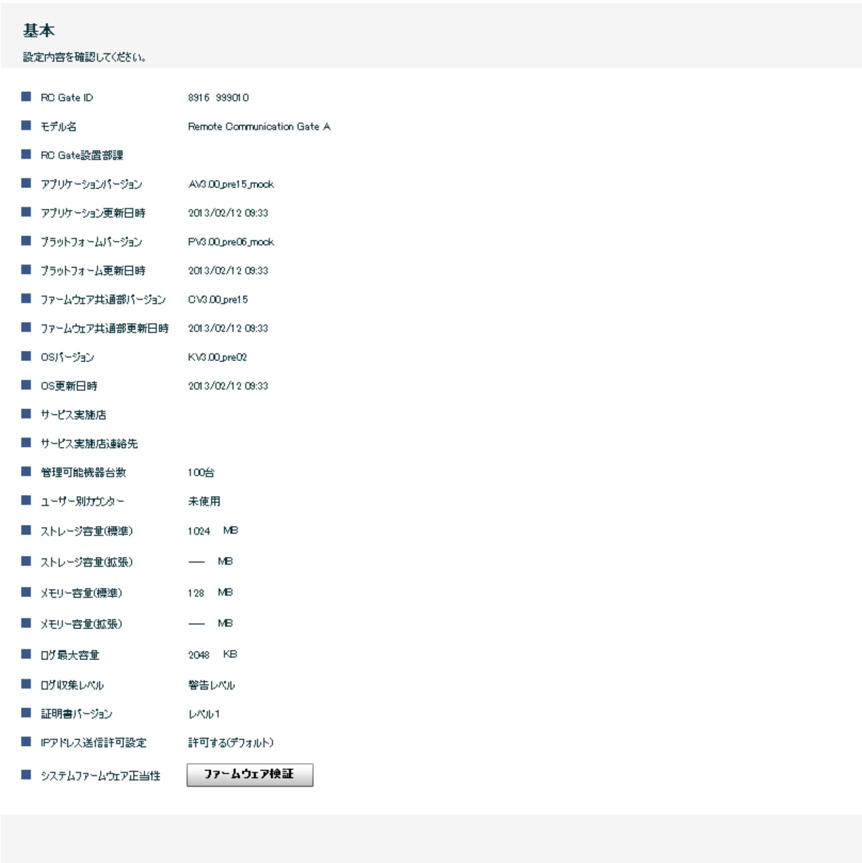
各画面に表示される項目の説明をします。

各画面に表示されるボタンの説明

ボタン名	ボタン概要
適用する	設定した内容を RC Gate に反映します。「日付・時刻」の設定では、時計のカウントが開始されます。
OK	確認ダイアログを表示します。
元に戻す	設定を変更せずに前の画面に戻ります。

基本

本機に関する基本情報を閲覧できます。[RC Gate 設定] - [基本] をクリックすると、本画面が表示されます。



項目名	項目説明
RC Gate ID	本機を識別するための番号です。製品ごとに振られた固有の番号です。
モデル名	本機のモデル名です。
RC Gate 設置部課	本機を設置した部課名・場所です。
アプリケーションバージョン	本機に内蔵されているアプリケーションのバージョンです。
アプリケーション更新日時	本機に内蔵されているアプリケーションの最終更新日時です。
プラットフォームバージョン	本機に内蔵されているアプリケーションを動作させるための、基盤ソフトウェアのバージョンです。
プラットフォーム更新日時	プラットフォームの最終更新日時です。
ファームウェア共通部バージョン	本機に内蔵されているアプリケーションが使用する共通のソフトウェアのバージョンです。
ファームウェア共通部更新日時	本機に内蔵されているアプリケーションが使用する共通のソフトウェアの、最終更新日時です。
OS バージョン	本機に内蔵されている OS のバージョンです。
OS 更新日時	本機に内蔵されている OS の最終更新日時です。
サービス実施店	本機の取扱店です。
サービス実施店連絡先	本機の取扱店の電話番号です。
管理可能機器台数	本機が管理できるデバイスの最大数です。
ユーザー別カウンター	ユーザー別のカウンター情報です。
ストレージ容量（標準）	拡張前のストレージ容量です。
ストレージ容量（拡張）	拡張後の追加分のストレージ容量です。
メモリー容量（標準）	拡張前のメモリー容量です。
メモリー容量（拡張）	拡張後の追加分のメモリー容量です。
ログ最大容量	本機が収集するログファイルの容量の最大値です。
ログ収集レベル	本機が収集するログのレベル（障害/警告/操作/情報）です。
証明書バージョン	本機が使用する証明書のバージョンです。
IP アドレス送信許可設定	RS センターシステムに本機とデバイスの IP アドレスの送信を許可したかどうかを表示します。
システムファームウェア正当性	［ファームウェア検証］をクリックし、本機に内蔵されたソフトウェアの正当性をチェックします。

日付・時刻

本機の時計の確認や変更ができます。［RC Gate 設定］-［日付・時刻］をクリックすると、本画面が表示されます。

重要

- 日付と時刻は定期的に確認し、必要に応じて正しく調整してください。



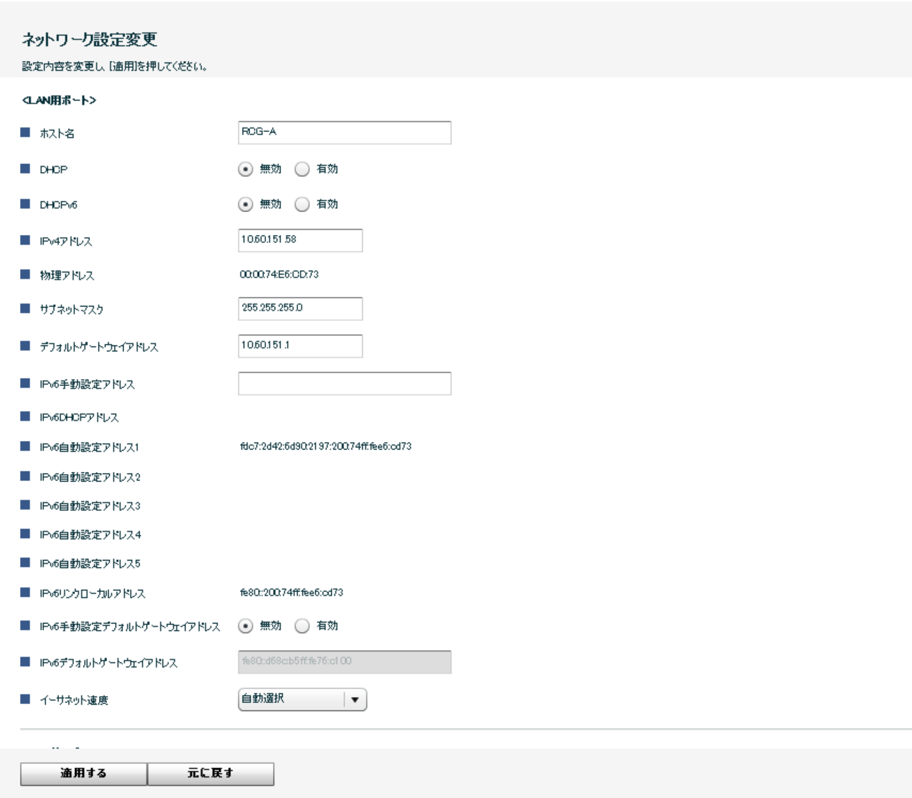
項目名	項目説明
タイムゾーン	本機を設置した場所の標準時間を、グリニッジ標準時からの差異で設定します。
年月日設定	本機を設置した場所の年月日を設定します。現在の日付を設定してください。
時刻設定	本機を設置した場所の時刻を設定します。現在の時刻を設定してください。

4

ネットワーク設定変更

本機のネットワーク設定の表示や変更ができます。[RC Gate 設定] - [ネットワーク] をクリックすると、本画面が表示されます。

ネットワークの設定を変更したあとは、再度ログインが必要です。画面に表示される URL をクリックして、Web ブラウザーを開きなおしてください。DHCP を使用した場合は、画面に表示される URL をアドレスバーに入力します。



<LAN 用ポート>

項目名	項目説明
ホスト名	本機のホスト名です。
DHCP	DHCP サーバーをご利用時は、[有効] に設定します。
DHCPv6	DHCPv6 サーバーをご利用時は、[有効] に設定します。
IPv4 アドレス	本機の LAN ポートの IPv4 アドレスです。「DHCP」欄が [有効] の場合は、DHCP サーバーから割り振られた本機の IPv4 アドレスを表示します。
物理アドレス	本機の LAN ポートの MAC アドレスです。

項目名	項目説明
サブネットマスク	本機の LAN ポートのサブネットマスクです。 DHCP 欄が［有効］の場合は、DHCP サーバーから取得した値を表示します。
デフォルトゲートウェイアドレス	本機が使用するゲートウェイのアドレスです。「DHCP」欄が［有効］の場合は、DHCP サーバーから取得された値を表示します。
IPv6 手動設定アドレス	本機の LAN ポートの IPv6 アドレスです。
IPv6 自動設定アドレス 1	本機の LAN ポートの IPv6 アドレスです。 「DHCPv6」 欄が［有効］の場合は、DHCP サーバーから取得された値を表示します。
IPv6 自動設定アドレス 2	本機の LAN ポートの IPv6 アドレスです。 「DHCPv6」欄が［有効］の場合は、DHCP サーバーから取得された値を表示します。
IPv6 自動設定アドレス 3	本機の LAN ポートの IPv6 アドレスです。 「DHCPv6」欄が［有効］の場合は、DHCP サーバーから取得された値を表示します。
IPv6 自動設定アドレス 4	本機の LAN ポートの IPv6 アドレスです。 「DHCPv6」欄が［有効］の場合は、DHCP サーバーから取得された値を表示します。
IPv6 自動設定アドレス 5	本機の LAN ポートの IPv6 アドレスです。 「DHCPv6」欄が［有効］の場合は、DHCP サーバーから取得された値を表示します。
IPv6 リンクローカルアドレス	本機の LAN ポートの IPv6 リンクローカルアドレスです。 「DHCPv6」欄が［有効］の場合は、DHCP サーバーから取得された値を表示します。
IPv6 手動設定デフォルトゲートウェイアドレス	本機が使用するゲートウェイの IPv6 アドレスです。
IPv6 デフォルトゲートウェイアドレス	本機が使用するゲートウェイの IPv6 アドレスです。 「DHCPv6」欄が［有効］の場合は、DHCP サーバーから取得された値を表示します。
イーサネット速度	本機の LAN ポートのイーサネット速度を選択します。

<DNS サーバー>

項目名	項目説明
プライマリ DNS サーバー	本機が主に使用する DNS サーバーの IP アドレスです。IP アドレスは、「x.x.x.x」形式（「x」は 0〜255 の範囲内の整数）で入力してください。

項目名	項目説明
セカンダリ DNS サーバー	プライマリ DNS サーバーが使用できず、セカンダリ DNS サーバーを使用する場合、セカンダリ DNS サーバーの IP アドレスを入力します。IP アドレスは、「x.x.x.x」形式（「x」は 0〜255 の範囲内の整数）で入力してください。

<IEEE802.1x 認証>

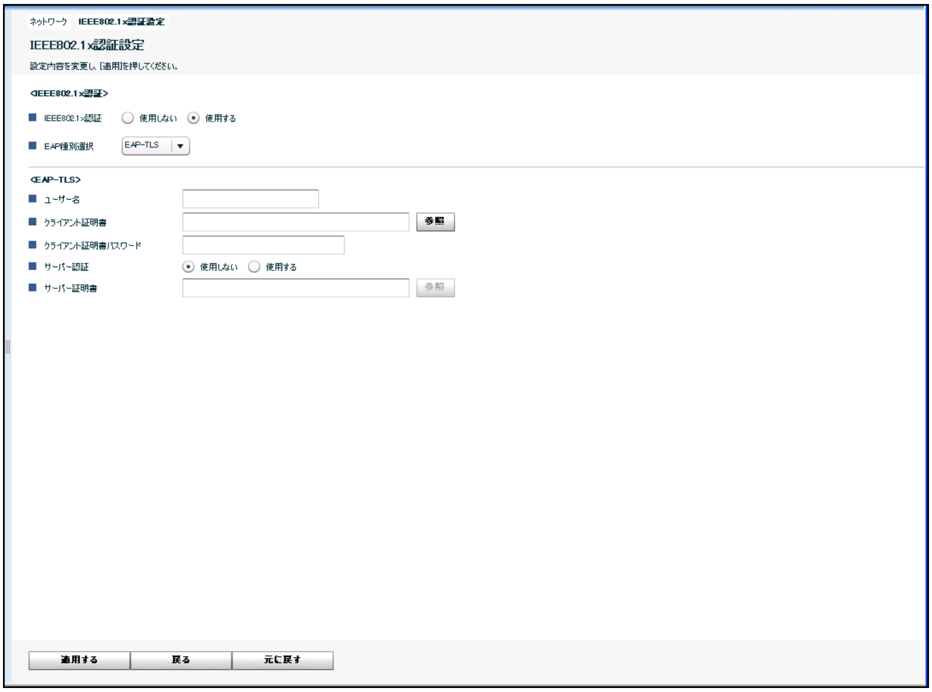
項目名	項目説明
IEEE802.1x 認証	IEEE802.1x 認証の設定を変更するときは［設定］をクリックし、設定画面を表示させます。

<メンテナンス用ポート>

項目名	項目説明
IP アドレス	PC ポート（メンテナンスポート）の IP アドレスです。ネットワーク環境により、本機の PC ポートの IP アドレスに 192.168.10.1 が利用できない場合は、サービス実施店にご連絡ください。
物理アドレス	PC ポートの MAC アドレスです。
サブネットマスク	PC ポートのサブネットマスクです。

IEEE802.1x 認証

IEEE802.1x のユーザー認証を使用するかどうか指定できます。［RC Gate 設定］-［ネットワーク設定］をクリックし、「< IEEE802.1x 認証>」欄の［設定］をクリックすると、本画面が表示されます。



<IEEE802.1x 認証>

項目名	項目説明
IEEE802.1x 認証	IEEE802.1x 認証を使用するかどうかを設定します。
EAP 種別選択	認証の種別を選択します。

<EAP-TLS>

項目名	項目説明
ユーザー名	認証サーバーへのログインユーザー名です。
ドメイン名	認証サーバーへのドメイン名を設定します。
クライアント証明書	クライアント証明書へのパスを入力するか、［参照］をクリックして、証明書を選択します。
クライアント証明書パスワード	サーバー認証有効時の証明書パスワードを入力します。サーバー認証を［使用する］にした場合だけ、表示されます。
サーバー認証	ルート認証によるサーバー認証を使用するかどうかを設定します。サーバー認証を［使用する］にした場合だけ、表示されます。
サーバー証明書	サーバー認証有効時のサーバー ID です。サーバー認証を［使用する］にした場合だけ、表示されます。

<PEAP>

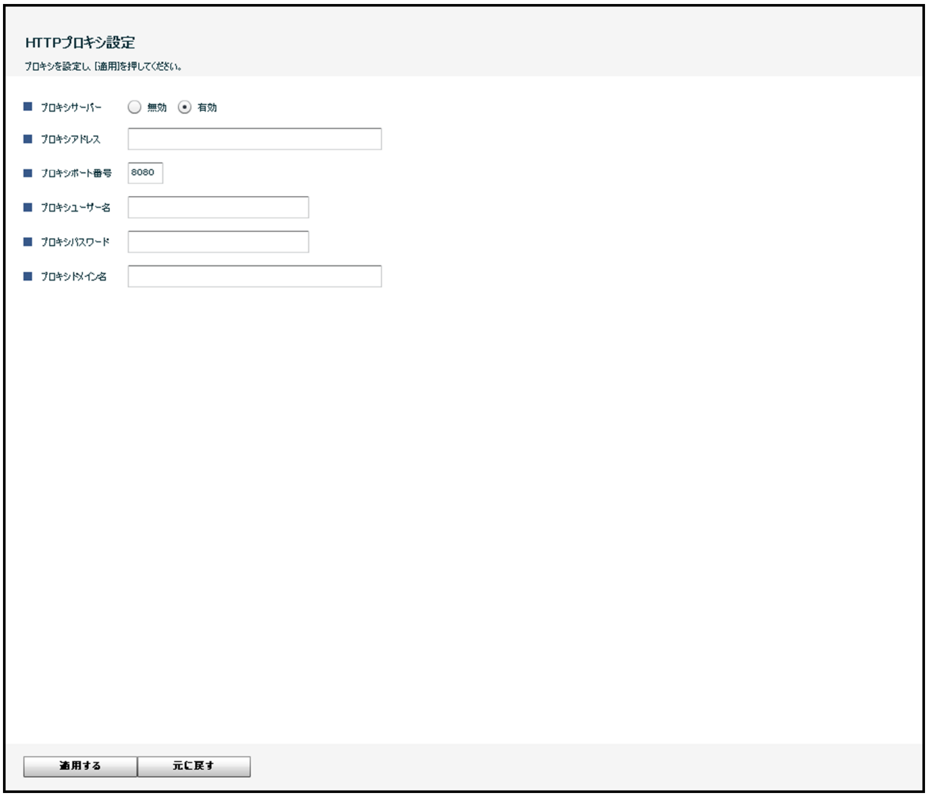
項目名	項目説明
ユーザー名	認証サーバーへのログインユーザー名です。
ドメイン名	認証サーバーへのドメイン名を設定します。
トンネリングユーザー名	トンネリング認証で使用するユーザー名を設定します。サーバー認証を［使用する］にした場合だけ、表示されます。
トンネリングパスワード	IEEE802.1x 認証を使用する場合は、証明書のパスを入力します。サーバー認証を［使用する］にした場合だけ、表示されます。
サーバー認証	ルート認証によるサーバー認証を使用するかどうかを設定します。サーバー認証を［使用する］にした場合だけ、表示されます。
サーバー証明書	サーバー認証有効時のサーバー ID です。サーバー認証を［使用する］にした場合だけ、表示されます。

<EAP-TTLS>

項目名	項目説明
ユーザー名	認証サーバーへのログインユーザー名です。
ドメイン名	認証サーバーへのドメイン名を設定します。
トンネリング方式	トンネリング方式を設定します。
トンネリングユーザー名	トンネリング認証で使用するユーザー名を設定します。サーバー認証を［使用する］にした場合だけ、表示されます。
トンネリングパスワード	IEEE802.1x 認証を使用する場合は、証明書のパスを入力します。サーバー認証を［使用する］にした場合だけ、表示されます。
サーバー認証	ルート認証によるサーバー認証を使用するかどうかを設定します。サーバー認証を［使用する］にした場合だけ、表示されます。
サーバー証明書	サーバー認証有効時のサーバー ID です。サーバー認証を［使用する］にした場合だけ、表示されます。

HTTP プロキシ設定

本機と RS センターシステムとの通信に、HTTP プロキシを使用するかどうか設定できます。［RC Gate 設定］-［HTTP プロキシ設定］をクリックすると、本画面が表示されます。



項目名	項目説明
プロキシサーバー	HTTP プロキシを有効にするかどうかを選択します。[有効] の場合は、以下の各項目を設定します。[無効] の場合は、以下の各項目の設定は不要です。
プロキシアドレス	HTTP プロキシを「x.x.x.x」形式（「x」は 0〜255 の範囲内の整数）で設定します。 HTTP プロキシサーバーをドメイン名で指定する場合：P.90「ネットワーク設定変更」を参照し、DNS サーバーを設定します。
プロキシポート番号	HTTP プロキシのポート番号を半角数字で入力します。工場出荷時の設定は 8080 です。
プロキシユーザー名	HTTP プロキシの認証用のユーザー名を 30 文字（ASCII 文字）以内で入力します。
プロキシパスワード	HTTP プロキシの認証用に、ユーザー名に対応するパスワードを 30 文字（ASCII 文字）以内で入力します。
プロキシドメイン名	「Windows 統合認証」（NTLMv2 認証だけ）を使用する場合は、ドメイン名を 255 文字（ASCII 文字）以内で入力します。

メール

本機が使用するメール設定情報の表示や変更ができます。[RC Gate 設定] - [メール] をクリックすると、本画面が表示されます。

重要

- 「RC Gate 管理者メールアドレス」宛てのメールは、プレーンテキストで送信されます。



<RC Gate メールアドレス>

項目名	項目説明
RC Gate メールアドレス（送信者用）	本機のメールアドレスです。下記メール発信時に使用します。 • 「センター接続休止/復旧通知」 • 「機器停止通知」 • 「機器ファームウェア更新通知」 デフォルト：rc_gate 126 文字（ASCII 文字）以内で入力します。
RC Gate メールアドレス（受信者用）	RC Gate への返信先のメールアドレスです。「RC Gate メールアドレス（送信者用）」と別のメールアドレスを設定できます。カンマ（,）で区切ることで、複数のメールアドレスを設定できます。255 文字（ASCII 文字）以内で入力します。
テストメール送信（ボタン）	設定確認のためのテストボタンです。クリックすると、「RC Gate 管理者メールアドレス」宛てにテストメールが送信されます。本項目は、本機の登録が完了するまでは表示されません。
RC Gate 管理者メールアドレス	「センター接続休止通知」や「センター接続復旧通知」メール等を受信する、本機の管理者のメールアドレスです。本項目は、本機の登録が完了するまでは表示されません。
メール再送信回数	メール送信が失敗したとき、SMTP サーバーへの接続を試みる回数を設定します。1〜60 回の範囲で設定できます。
メール再送信間隔時間	メール送信が失敗したとき、SMTP サーバーへの接続を試みる期間を設定します。1〜60 秒の範囲で設定できます。

<SMTP サーバー>

項目名	項目説明
SMTP サーバーアドレス	以下の内容のメールを管理者宛てに送信する際に使用する、IP アドレスを指定します。 • センター接続休止/復旧 • 機器停止 • 機器ファームウェア更新 IP アドレスで指定する場合：「x.x.x.x」形式（「x」は 0〜255 の範囲内の整数）で設定します。 SMTP サーバーをドメイン名で指定する場合：P.90「ネットワーク設定変更」を参照し、DNS サーバーを設定します。
SMTP サーバーポート番号	SMTP サーバーが使用するポート番号です。 通常は 25 を指定します。

項目名	項目説明
SMTP_AUTH	お使いの SMTP サーバーが SMTP 認証を使用している場合は、［有効］を選択します。SMTP サーバーが SMTP 認証を使用していない場合、または POP before SMTP 認証を使用している場合は、［無効］を選択します。
SMTP_AUTH 認証方式	SMTP_AUTH を［有効］に設定する場合は、本項目を設定します。［自動］、［DIGEST-MD5］、［CRAM-MD5］、［LOGIN］および［PLAIN］から選択します。
ユーザー名	SMTP_AUTH の認証方式で使用するユーザー名（ユーザーID）です。通常は、「RC Gate メールアドレス（送信者用）」と同じアドレスが適用されますが、セキュリティ上の理由で別のアドレスが適用される場合もあります。
パスワード	SMTP_AUTH の認証方式で使用するパスワードを入力します。通常は、「RC Gate メールアドレス（送信者用）」と同じパスワードが適用されますが、セキュリティ上の理由で別のパスワードが適用される場合もあります。

<POP サーバー>

項目名	項目説明
POP before SMTP	お使いの SMTP サーバーが POP before SMTP 認証を使用している場合は、［有効］を選択します。SMTP 認証を使用していない場合、または SMTP_AUTH の認証方式を使用している場合は、［無効］を選択します。
POP サーバーアドレス	「POP before SMTP」認証を使用する場合の IP アドレスまたは POP サーバー名です。
POP サーバーポート番号	POP before SMTP 認証を使用している POP サーバーのポート番号です。通常は 110 に設定します。
ユーザー名	POP before SMTP 認証で使用するユーザー名（ユーザーID）です。
パスワード	POP before SMTP 認証で使用するパスワードです。
認証後待機時間	POP before SMTP 認証でエラーが発生した場合、待ち時間を長く設定してください。待ち時間は 0〜30 秒の範囲で設定してください。

補足

- 管理者に送信されるメールの内容については、『セットアップガイド』を参照してください。

メール送信の確認

次の手順で、メールが正しく送信できるかご確認ください。

設定を行う前に、SMTP サーバーの認証方式について、ネットワーク管理者にお問い合わせください。

1. [テストメール送信] をクリックする。

2. 管理者のメールソフトにて、テストメールが届いているか確認する。

届いている場合は、その設定で運用してください。

テストメールが届かなかった場合は、「RC Gate メールアドレス（送信者用）」欄に管理者のメールアドレスを入力し、手順 1〜2 を繰り返します。

試行の結果、テストメールが届かなかった場合は、サービス実施店にご連絡ください。

補足

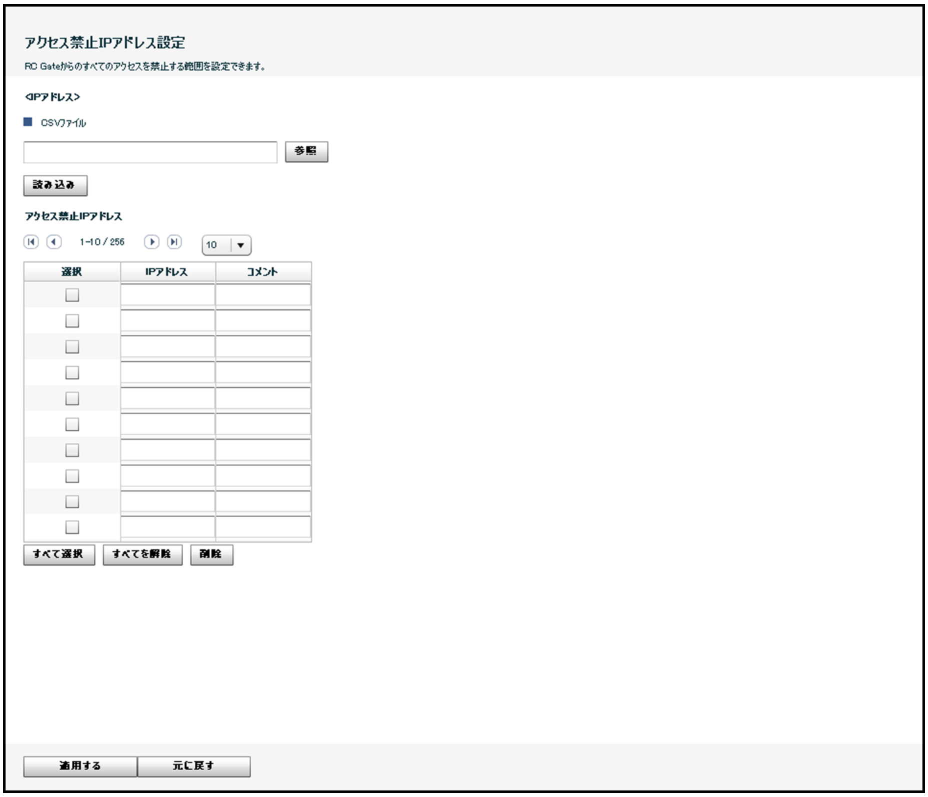
- メールアドレスは、@マーク以降の文字も入力してください。
- POP before SMTP 認証でエラーが発生した場合、「認証後待機時間」をさらに長めに設定してください。

アクセス禁止 IP アドレス

本機からアクセスを禁止するデバイスの IP アドレスを指定できます。[RC Gate 設定] - [アクセス禁止 IP アドレス] をクリックすると、本画面が表示されます。

重要

- **本機からのアクセスを禁止したデバイスの IP アドレスが DHCP 方式で割り当てられると、管理対象であるべきデバイスの情報も収集できなくなります。**



<IP アドレス>

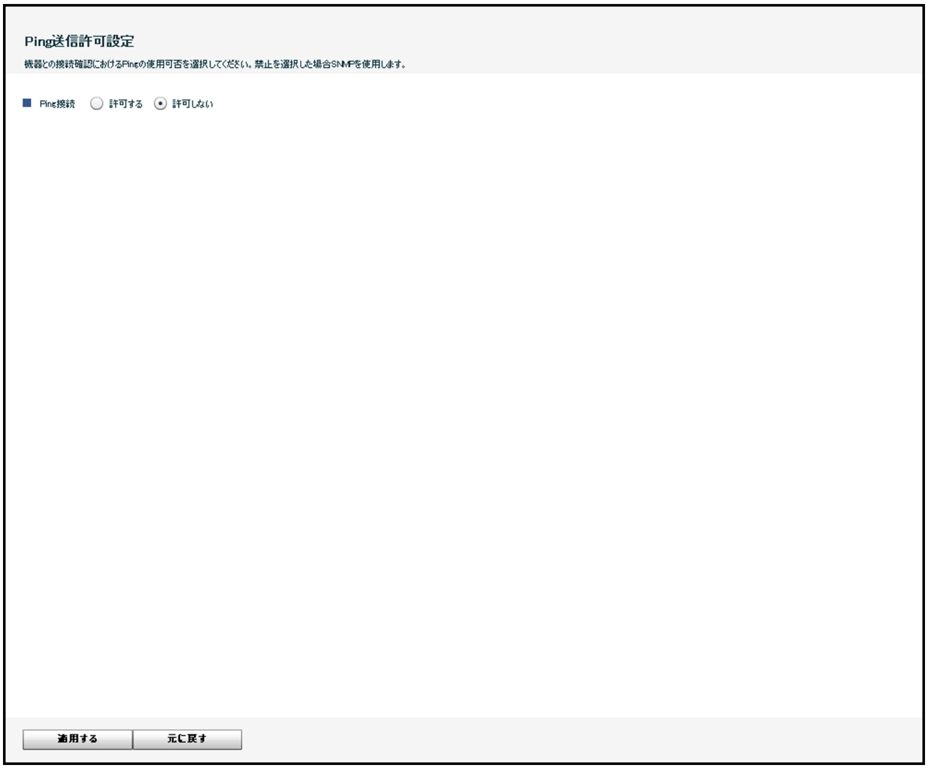
項目名	項目説明
CSV ファイル	インポートする CSV ファイルを指定します。
参照（ボタン）	インポートする CSV ファイルの場所を指定します。
読み込み（ボタン）	指定した CSV ファイルのインポートを開始します。

アクセス禁止 IP アドレス

項目名	項目説明
IP アドレス	本機からのアクセスを禁止するデバイスの、IP アドレスを入力します。
コメント	デバイスのコメント情報です。61 文字（ASCII 文字）以内で設定します。
すべて選択（ボタン）	リスト内の項目をすべて選択します。
すべてを解除（ボタン）	リスト内の項目の選択をすべて解除します。
削除（ボタン）	選択した項目をすべて削除します。

Ping 送信許可設定

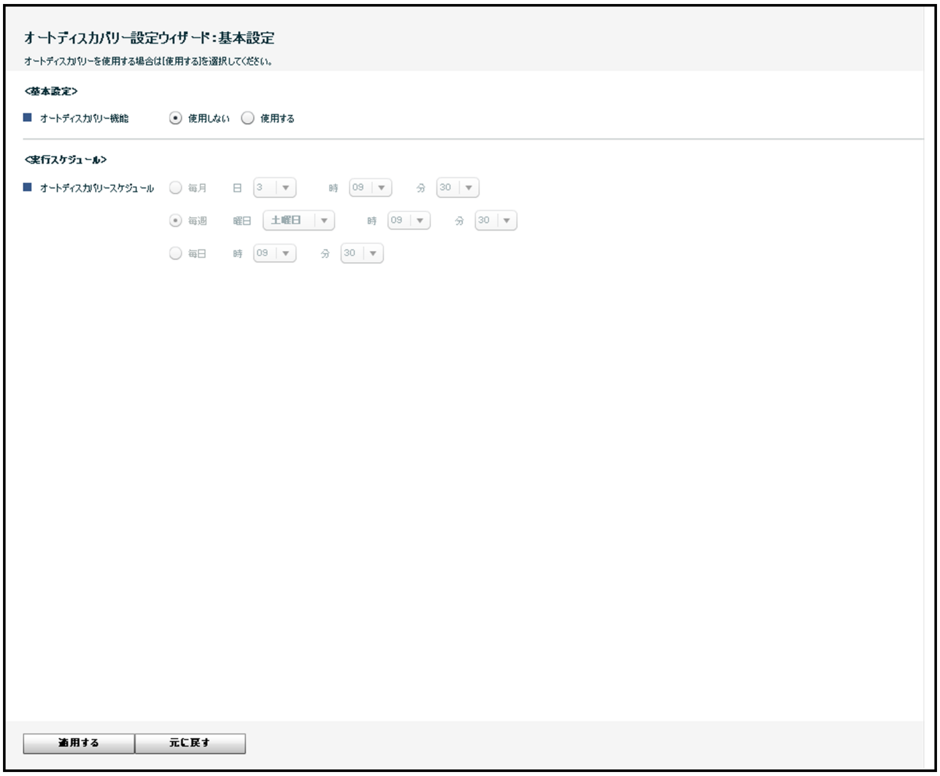
デバイス検索時に Ping 送信を許可するかどうかを設定できます。[RC Gate 設定] - [Ping 接続] をクリックすると、本画面が表示されます。



項目名	項目説明
Ping 接続	Ping 送信を禁止する場合は [許可しない] を選択します。[許可しない] に設定した場合は、Ping の代わりに SNMP を使用します。

オートディスカバリー基本設定

オートディスカバリーの基本的な設定について、説明します。[オートディスカバリー] - [基本設定] をクリックすると、本画面が表示されます。



項目名	項目説明
オートディスカバリー機能	オートディスカバリーを使用するかどうかを設定します。工場出荷時の設定は、[使用しない] です。
オートディスカバリースケジュール	オートディスカバリーを実行するスケジュールを設定します。工場出荷時の設定は、[毎月] です。

オートディスカバリープロトコル設定

オートディスカバリーで使用するプロトコルの情報を設定します。[オートディスカバリー] - [プロトコル設定] をクリックすると、本画面が表示されます。

4



項目名	項目説明
使用プロトコル	有効にする SNMP プロトコルを設定します。工場出荷時の設定は、[SNMPv1,v2] です。
SNMP コミュニティ名	SNMP 対応機検索に使用するコミュニティ名を設定します。コミュニティ名は、SNMP 対応機に問い合わせをするときにパスワードのような働きをするもので、SNMP 対応機側で設定されています。工場出荷時の設定は、「public」です。 各コミュニティ名を 30 文字(ASCII 文字)以内で入力します。
ユーザー名	SNMP 認証方式で使用するユーザー名です。工場出荷時は、設定されていません。 設定する場合は、32 文字(ASCII 文字)以内で入力します。
認証用パスワード	SNMP 認証方式で使用する「ユーザー名」のパスワードを入力します。工場出荷時は、設定されていません。 設定する場合は、32 文字(ASCII 文字)以内で入力します。
認証プロトコル	SNMP 認証方式で使用するプロトコルを設定します。

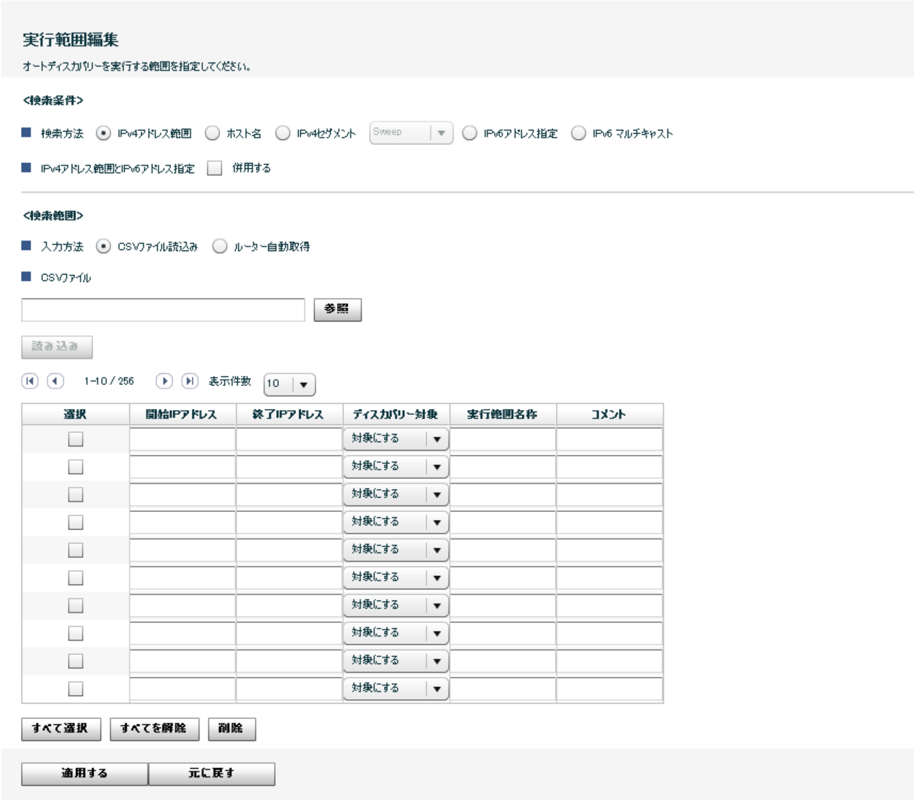
項目名	項目説明
暗号化パスワード	SNMP 認証方式で使用する暗号化されたパスワードを入力します。工場出荷時は、設定されていません。 設定する場合は、32 文字（ASCII 文字）以内で入力します。
暗号化プロトコル	SNMP 認証方式で使用する暗号化されたプロトコルを設定します。
コンテキスト名	SNMPv3 設定で使用するコンテキスト名です。32 文字（ASCII 文字）以内で入力します。

オートディスカバリーの実行範囲設定

ネットワーク上にあるデバイスのうち、オートディスカバリーを行う範囲を指定できます。［オートディスカバリー］-［実行範囲編集］をクリックすると、本画面が表示されます。

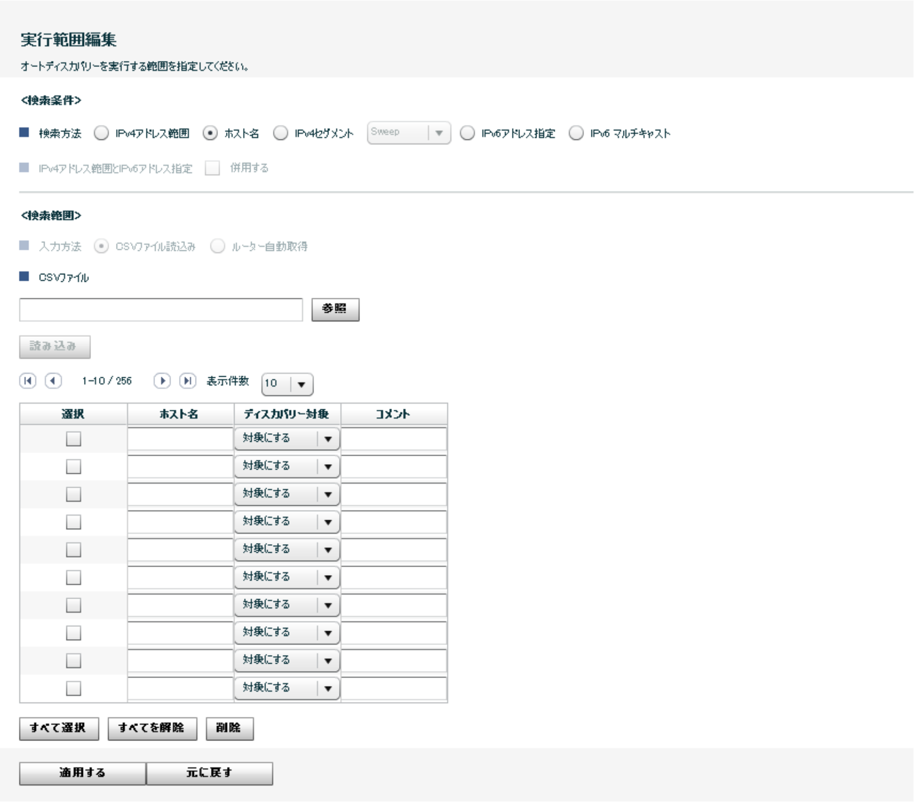
項目名	項目説明
検索方法	［IP v4 アドレス範囲］、［ホスト名］、［IP v4 セグメント］、［IPv6 アドレス指定］、または、［IPv6 マルチキャスト］を選択し、検索する方法を設定します。［IPv4 セグメント］を指定した場合は、［Sweep］または、［Broadcast］を選択します。
IPv4 アドレス範囲と IPv6 アドレス指定	IPv4 アドレス範囲と IPv6 アドレス指定の両方を使って指定する場合は、［併用する］を選択します。
入力方法	［IP v4 アドレス範囲］または［IP v4 セグメント］を指定した場合は、［CSV ファイル読込み］または［ルーター自動取得］を選択し、入力方法を設定します。
CSV ファイル	CSV ファイルを指定し、IP アドレスを設定します。
参照（ボタン）	クリックしてインポートする CSV ファイルの場所を指定します。
読み込み（ボタン）	クリックすると、指定した CSV ファイルのインポートを開始します。
検索ホップ数（0-10）	［ルーター自動取得］を選択した場合に、問い合わせるルーターの深度（どの階層のルーターまで問い合わせを行うか）を入力します。
アクセス禁止 IP アドレス設定へ（ボタン）	「アクセス禁止 IP アドレス設定」画面を表示します。本機からアクセスを禁止するデバイスの IP アドレスを設定できます。詳細は、P.99「アクセス禁止 IP アドレス」を参照してください。

IPv4 アドレス範囲を選択した場合



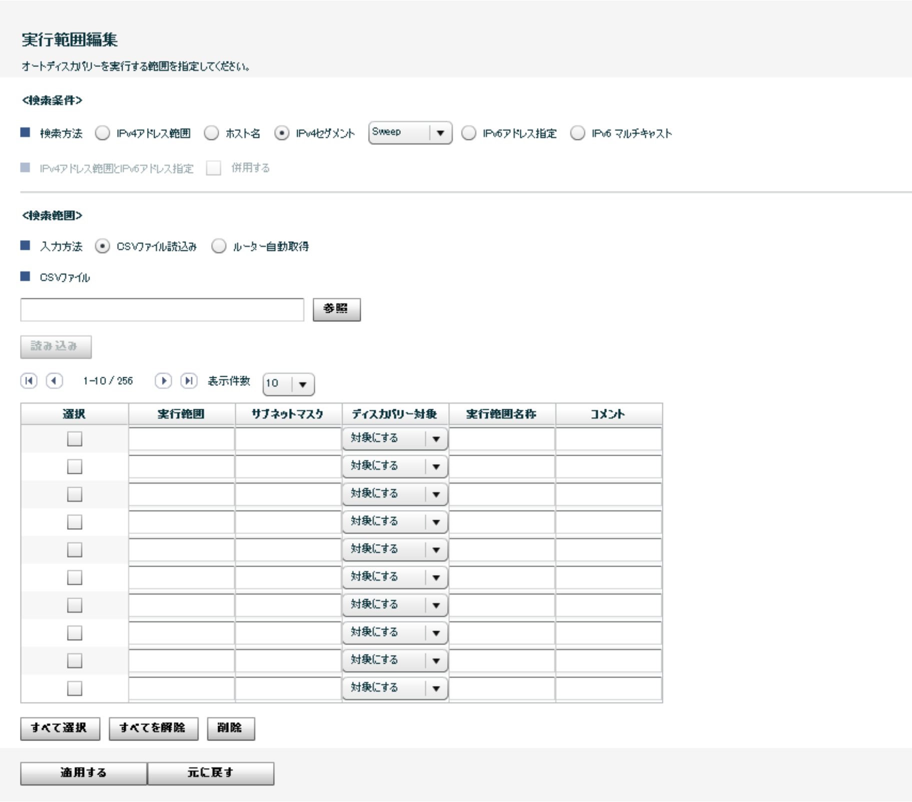
Item	Descriptions
開始 IP アドレス	デバイスの検索を開始する IPv4 アドレスを指定します。IP v4 アドレスを「x.x.x.x」形式（「x」は 0～255 の範囲内の整数）で入力します。
終了 IP アドレス	デバイスの検索を終了する IP v4 アドレスを指定します。IP v4 アドレスを「x.x.x.x」形式（「x」は 0～255 の範囲内の整数）で入力します。
ディスカバリー対象	オートディスカバリー実行の対象とするかどうかを選択します。
実行範囲名称	「実行範囲」の IP v4 アドレスに対し、ネットワークアドレス名を 61 文字（ASCII 文字）以内で入力します。
コメント	「実行範囲」の各 IP v4 アドレスに対し、コメントを 61 文字（ASCII 文字）以内で入力します。
すべて選択（ボタン）	リスト内の項目をすべて選択します。
すべてを解除（ボタン）	リスト内の項目の選択をすべて解除します。
削除（ボタン）	選択した項目をすべて削除します。

ホスト名を選択した場合



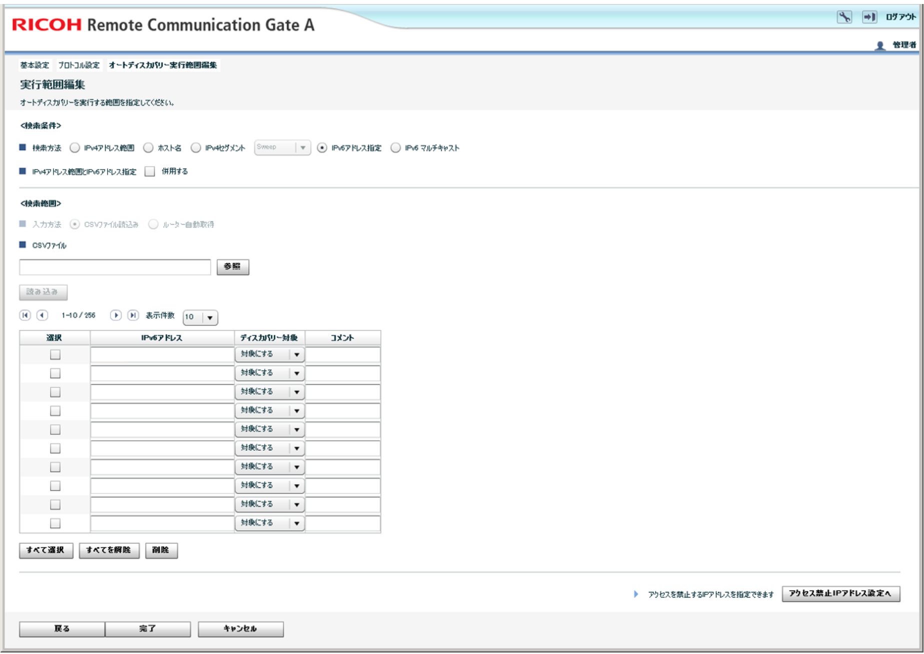
Item	Descriptions
ホスト名	検索するデバイスのホスト名を指定します。
ディスカバリー対象	オートディスカバリー実行の対象とするかどうかを選択します。
コメント	ホスト名に対し、コメントを 61 文字（ASCII 文字）以内で入力します。

IPv4 セグメントを選択した場合



Item	Descriptions
実行範囲	オートディスカバリーに使用するネットワークアドレスです。IPv4 アドレスを「x.x.x.x」形式（「x」は 0〜255 の範囲内の整数）で入力します。
サブネットマスク	実行範囲を指定するサブネットマスクです。サブネットマスクを「x.x.x.x」形式（「x」は 0〜255 の範囲内の整数）で入力します。
ディスカバリー対象	オートディスカバリー実行の対象とするかどうかを選択します。
実行範囲名称	「実行範囲」の IPv4 アドレスに対し、ネットワークアドレス名を入力します。
コメント	「実行範囲」の各 IPv4 アドレスに対し、コメントを 61 文字（ASCII 文字）以内で入力します。
すべて選択（ボタン）	リスト内の項目をすべて選択します。
すべてを解除（ボタン）	リスト内の項目の選択をすべて解除します。
削除（ボタン）	選択した項目をすべて削除します。

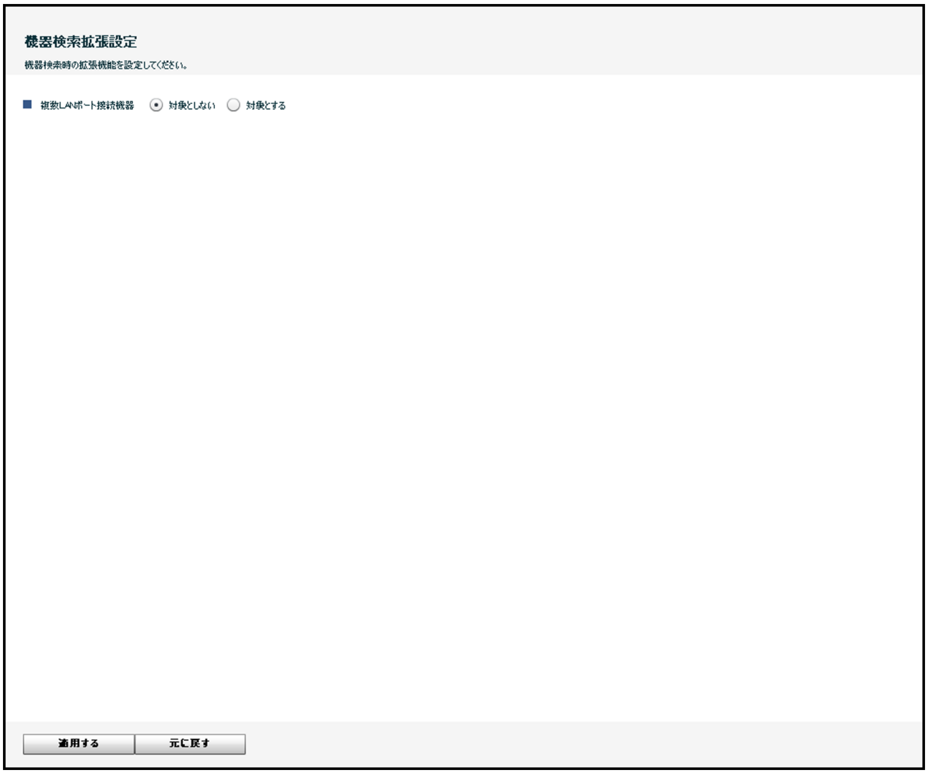
IPv6 アドレス指定を選択した場合



Item	Descriptions
IPv6 アドレス	検索するデバイスの IPv6 アドレスを指定します。「xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx」形式で 16 進数を入力します。
ディスカバリー対象	オートディスカバリー実行の対象とするかどうかを選択します。
コメント	IPv6 アドレスに対し、コメントを 61 文字（ASCII 文字）以内で入力します。

機器検索拡張設定

デバイスの検索範囲を拡張するかどうかを指定できます。[機器管理] - [機器検索拡張設定] をクリックすると、本画面が表示されます。



Item	Descriptions
複数 LAN ポート接続機器	以下のデバイスは、オートディスカバリーで検出されない場合があります。 • プリンター機能が搭載されていない Ricoh デバイス • 複数のネットワークインターフェースが搭載されたデバイス 上記のデバイスは、本機能を有効すると見つかる場合があります。ただし、有効にすると検索に時間がかかります。詳細は、サービス実施店にご相談ください。

登録機器一覧

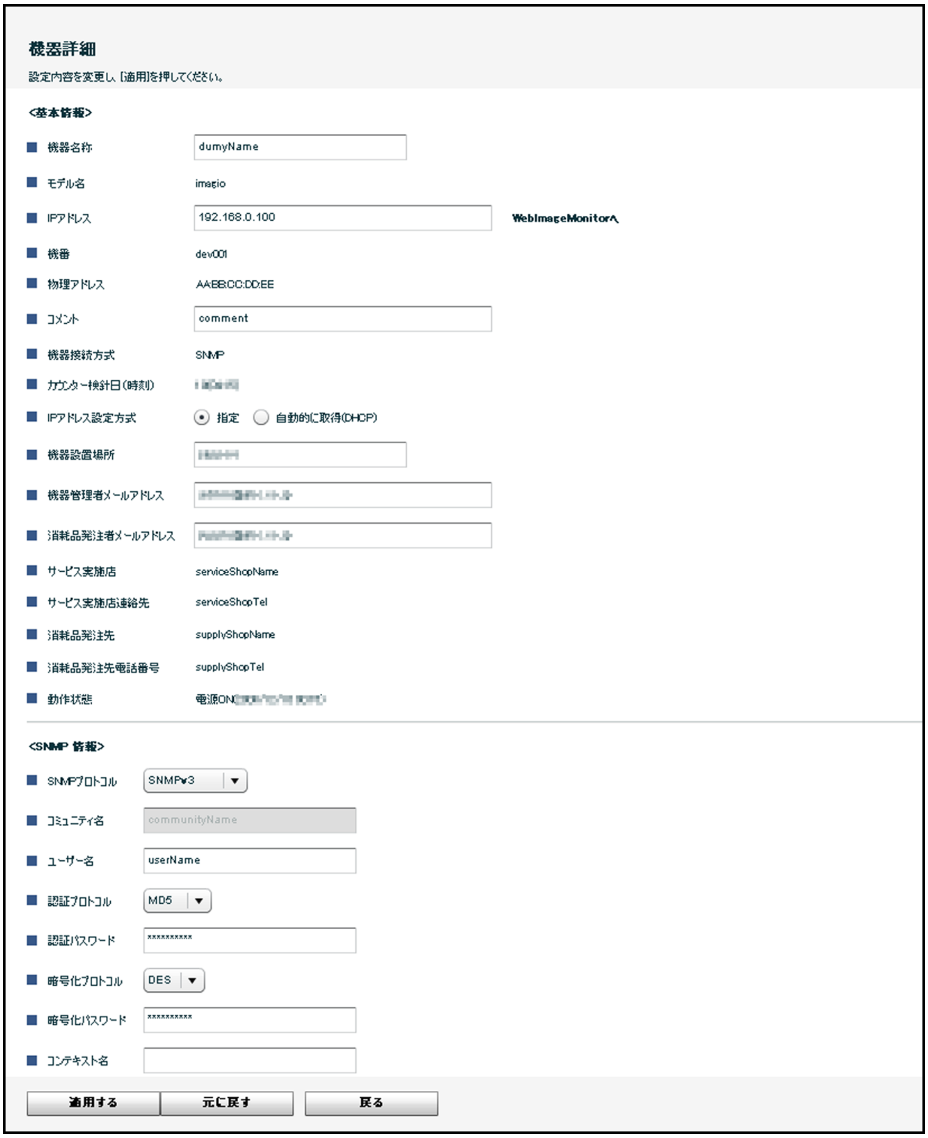
本機が管理しているデバイスの一覧表です。[機器管理] - [登録機器一覧] をクリックすると、本画面が表示されます。[最新の情報に更新] をクリックすると、最新情報が表示されます。



項目名	項目説明
モデル名	デバイスのモデル名です。モデル名が取得できない場合は「---」で表示されます。
アドレス	デバイスの IPv4 アドレス、IPv6 アドレス、またはホスト名です。
機番	デバイスの機番です。 をクリックすると、「機器詳細」画面が表示されます。
機器設置場所	デバイスが設置されている場所です。
コメント	デバイスのコメント情報です。

機器詳細

本機が管理しているデバイスの詳細な情報の表示や変更ができます。[機器管理] - [登録機器一覧] をクリックし、機番のをクリックすると、本画面が表示されます。



項目名	項目説明
機器名称	デバイスの名称です。変更する場合は 30 文字（ASCII 文字）以内で設定します。
モデル名	デバイスのモデル名です。
IPv4 アドレス	デバイスの IPv4 アドレスです。
IPv6 アドレス	バイスの IPv6 アドレスです。
ホスト名	デバイスのホスト名です。
機番	デバイスの機番です。

項目名	項目説明
物理アドレス	デバイスの MAC アドレスです。
コメント	デバイスのコメント情報です。61 文字（ASCII 文字）以内で設定します。
機器接続方式	デバイスの接続方式です。
カウンター検針日（時刻）	カウンターの検針日と時刻です。
IP アドレス設定方式	ネットワーク上のデバイスの IP アドレスの取得方式を設定します。[指定]、[自動的に取得（DHCP）] から選択します。
機器設置場所	デバイスが設置されている場所を設定します。変更する場合は 30 文字（ASCII 文字）以内で設定します。
機器管理者メールアドレス	デバイスの管理者のメールアドレスです。「機器ファームウェア更新通知」メールや「機器停止通知」メール等の宛て先となります。120 文字（ASCII 文字）以内で設定します。
消耗品発注者メールアドレス	デバイスの消耗品を発注する担当者のメールアドレスです。120 文字（ASCII 文字）以内で設定します。 ただし、サービスの内容・地域によっては表示されない場合があります。
サービス実施店	デバイスの取扱店を表示します。
サービス実施店連絡先	デバイスの取扱店の連絡先電話番号です。
消耗品発注先	デバイスの消耗品の取扱店です。 ただし、サービスの内容・地域によっては表示されない場合があります。
消耗品発注先電話番号	デバイスの消耗品の取扱店の連絡先電話番号です。ただし、サービスの内容・地域によっては表示されない場合があります。
動作状態	デバイスの動作状態です。

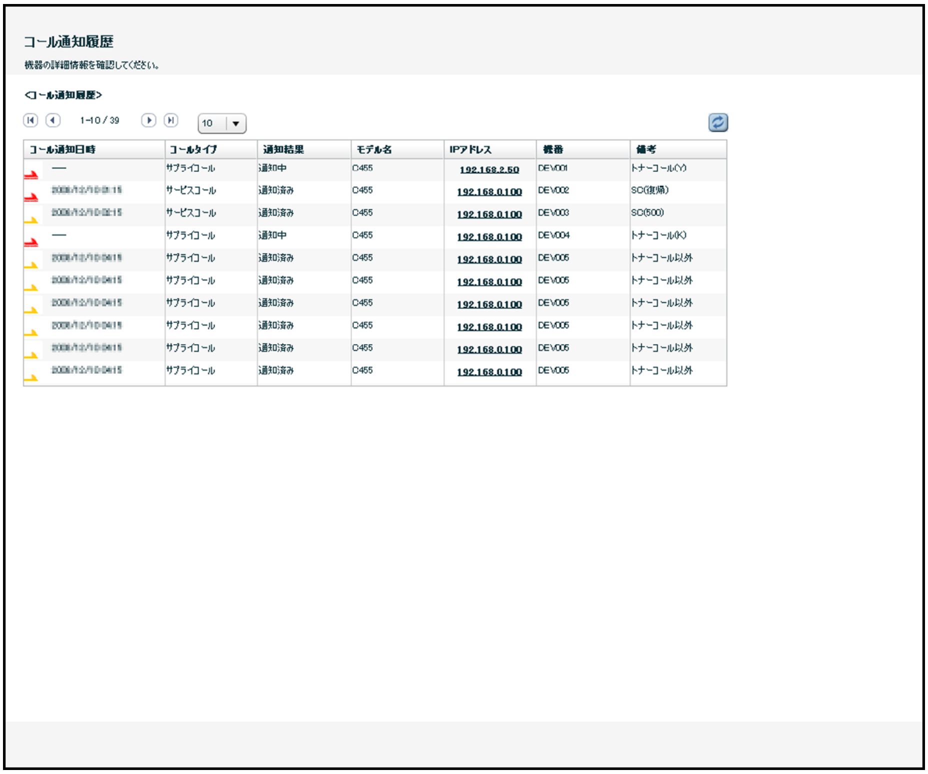
SNMP 情報

項目名	項目説明
SNMP プロトコル	現在有効な SNMP プロトコルを設定します。
コミュニティ名	SNMP プロトコルで情報を取得する SNMP 対応機の場合のコミュニティ名です。変更する場合は 30 文字（ASCII 文字）以内で設定します。工場出荷時の設定は Public です。
ユーザー名	SNMP 認証方式で使用するログインユーザー名です。変更する場合は 32 文字（ASCII 文字）以内で設定します。
認証プロトコル	SNMP 認証方式で使用するプロトコルを設定します。

項目名	項目説明
認証パスワード	SNMP 認証方式で使用する「ユーザー名」のパスワードを 32 文字（ASCII 文字）以内で入力します。
暗号化プロトコル	SNMP 認証方式で使用する暗号化されたプロトコルを設定します。
暗号化パスワード	SNMP 認証方式で使用する暗号化されたパスワードを 32 文字（ASCII 文字）以内で入力します。
コンテキスト名	SNMPv3 設定で使用するコンテキスト名です。最大で 32 文字（ASCII 文字）入力できます。

コール通知履歴

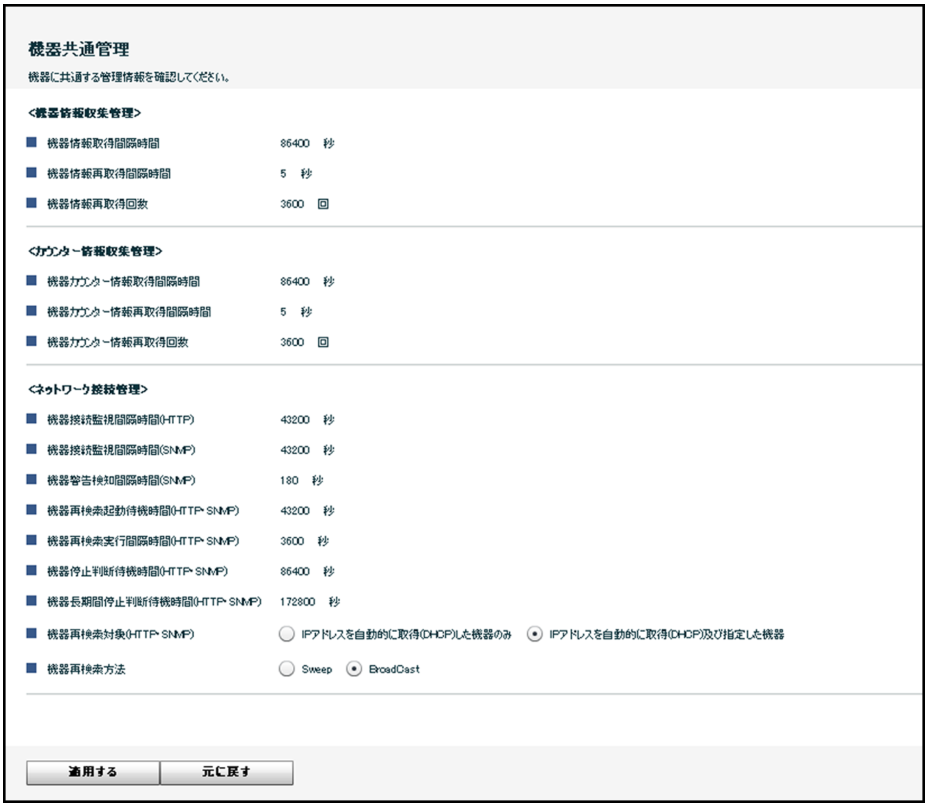
コールを通知した日付、コール種別、コールが発生したデバイス情報を表示します。通知履歴は 100 件まで保持できます。［機器管理］-［登録機器一覧］-［コール通知履歴］をクリックすると、本画面が表示されます。



項目名	項目説明
コール通知日時	デバイスからのコールが RS センターシステムに通知された日時を表示します。 • 1 時間以内に通知されたコールと、「通知結果」が「通報中」のコールは、赤で表示されます。 • 24 時間以内に通知されたコールは、黄色で表示されます。
コールタイプ	コールタイプを表示します。 • サービスコール • マニュアルコール • サプライコール
通知結果	RS センターシステムへの通知結果を表示します。 • 成功 • 失敗 • サービス時間外 • 通知失敗 • 通報中
モデル名	コールが発生したデバイスのモデル名です。
IP アドレス	コールが発生したデバイスの IP アドレスです。
機番	コールが発生したデバイスの ID です。
備考	サービスコール番号や、サプライコールの詳細です。

機器共通管理

デバイスを管理するための各種動作設定を閲覧できます。[機器管理] - [機器共通管理] をクリックすると、本画面が表示されます。



<機器情報収集管理>

項目名	項目説明
機器情報取得間隔時間	デバイスのデータを取得する間隔です。
機器情報再取得間隔時間	デバイスのデータが正常に取得できなかったときに、再試行する間隔です。
機器情報再取得回数	デバイスのデータが正常に取得できなかったときに、再試行する回数です。

<カウンター情報収集管理>

項目名	項目説明
機器カウンター情報取得間隔時間	デバイスのカウンタデータを取得する間隔です。
機器カウンター情報再取得間隔時間	デバイスのカウンタデータが正常に取得できなかったときに、再試行する間隔です。
機器カウンター情報再取得回数	デバイスのカウンタデータが正常に取得できなかったときに、再試行する回数です。

<ネットワーク接続管理>

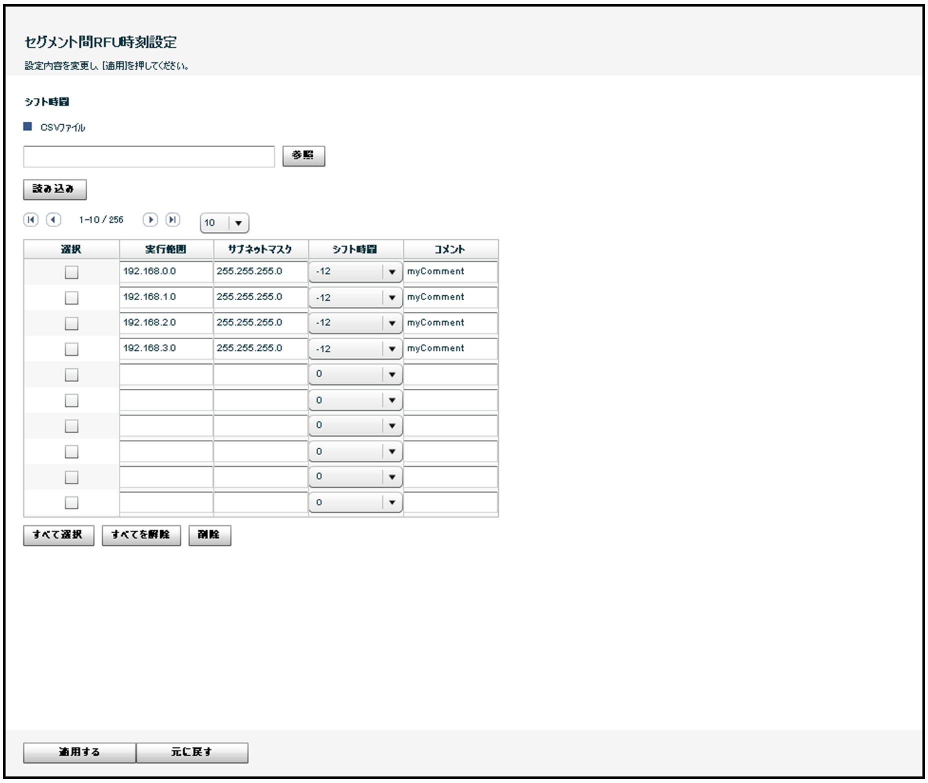
項目名	項目説明
機器接続監視間隔時間（HTTP）	HTTP プロトコルで情報を取得する HTTPS 対応機が接続されているかチェックする間隔です。
機器接続監視間隔時間（SNMP）	SNMP プロトコルで情報を取得する SNMP 対応機が接続されているかチェックする間隔です。
機器警告検知間隔時間（SNMP）	SNMP プロトコルで情報を取得する SNMP 対応機のアラートを検知する間隔です。
機器再検索起動待機時間（HTTP・SNMP）	ネットワーク上のデバイスを見失ってから、デバイスの再検索を実行するまでの時間です。
機器再検索実行間隔時間（HTTP・SNMP）	ネットワーク上のデバイスの再検索を開始後、次の再検索を実行するまでの間隔です。
機器停止判断待機時間（HTTP・SNMP）	ネットワーク上のデバイスを見失ってから、停止していると判断するまでの時間です。
機器長期間停止判断待機時間（HTTP・SNMP）	ネットワーク上のデバイスを見失ってから、長期間停止していると判断するまでの時間です。
機器再検索対象（HTTP・SNMP）	ネットワーク上のデバイスの再検索を実行する際、［IP アドレスを自動的に取得（DHCP）した機器のみ］、［IP アドレスを自動的に取得（DHCP）及び指定した機器］から選択します。 変更する場合は、サービス実施店にご連絡ください。
機器再検索方法	ネットワーク上のデバイスを見失った際の、再検索方法です。

機器ファームウェア更新時刻シフト

時差や業務開始時刻の違いなどを考慮し、デバイスのファームウェアを更新する時刻をセグメントごとに変更できます。［機器管理］-［機器ファームウェア更新時刻シフト］をクリックすると、本画面が表示されます。

最大で 256 セグメント設定できます。

パソコンに保存された CSV ファイルからセグメント情報をインポートできます。ネットワークアドレス、サブネットマスク、シフト時間、コメントをカンマ（,）で区切って入力してください。

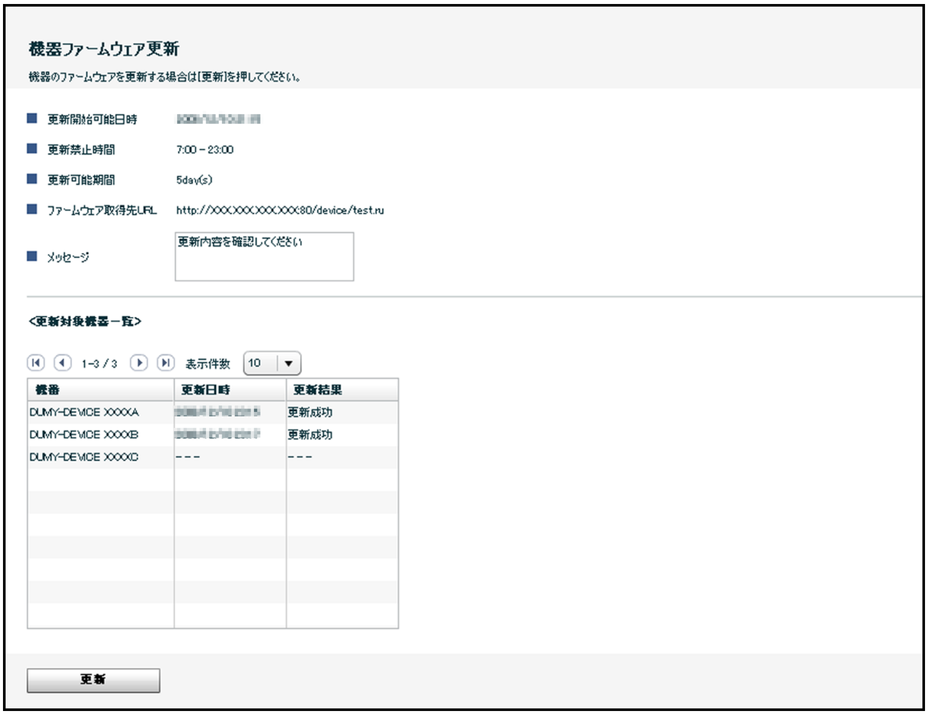


項目名	項目説明
CSV ファイル	インポートする CSV ファイルを指定します。
参照（ボタン）	クリックしてインポートする CSV ファイルの場所を指定します。
読み込み（ボタン）	クリックすると、指定した CSV ファイルのインポートを開始します。
実行範囲	ファームウェア更新時刻を変更するセグメントのネットワークアドレスを設定します。
サブネットマスク	ファームウェア更新時刻を変更するセグメントのサブネットマスクを設定します。
シフト時間	ファームウェア更新開始のシフトを設定します。-12〜+12 時間まで 1 時間刻みで設定できます。
コメント	デバイスのコメント情報を設定します。61 文字（ASCII 文字）以内で設定します。
すべて選択（ボタン）	リスト内の項目をすべて選択します。
すべてを解除（ボタン）	リスト内の項目の選択をすべて解除します。
削除（ボタン）	選択した項目をすべて削除します。

機器ファームウェア更新

デバイスのファームウェアの更新や、更新スケジュールの表示ができます。

[機器管理] - [機器ファームウェア更新] をクリックすると、本画面が表示されます。また、管理者宛てに届く「機器ファームウェア更新通知」メール内の URL リンクをクリックすると、RC Gate モニターが起動し、ログイン後すぐに本画面が表示されます。



項目名	項目説明
更新（ボタン）	ファームウェアを更新します。 更新スケジュールがない場合や、スケジュール実行中、スケジュール実行可能日前の場合、本ボタンは表示されません。
更新開始可能日時	デバイスのファームウェアの更新を開始できる日時を表示します。
更新禁止時間	ファームウェアの更新を禁止したい日時を表示します。
更新可能期間	デバイスのファームウェアを更新できる有効期間を表示します。この期間内に更新が完了しない場合は、更新失敗とみなされます。
ファームウェア取得先 URL	デバイスのファームウェアを取得する URL 先を表示します。
メッセージ	RS センターシステムからのメッセージを表示します。

機器ファームウェア更新前回履歴

機器ファームウェア更新の前回履歴を表示します。［機器管理］-［機器ファームウェア更新前回履歴］をクリックすると、本画面が表示されます。



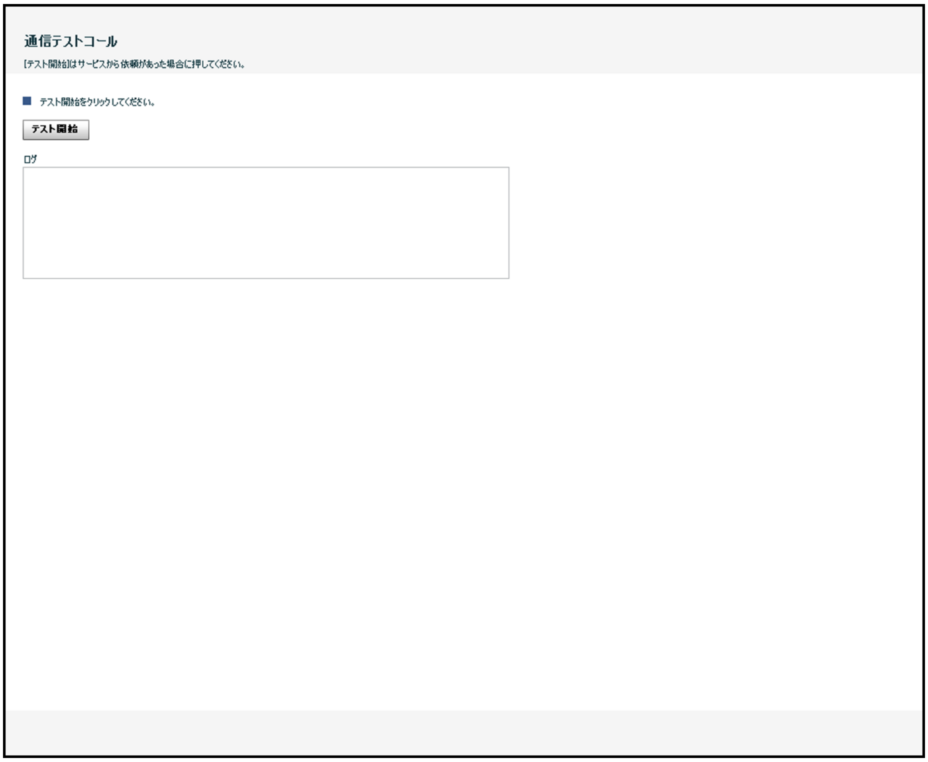
項目名	項目説明
更新開始可能日時	デバイスのファームウェアの更新を開始できる日時を表示します。
更新禁止時間	ファームウェアの更新を禁止したい日時を表示します。
更新可能期間	デバイスのファームウェアを更新できる有効期間を表示します。
ファームウェア取得先 URL	デバイスのファームウェアを取得する URL 先を表示します。
メッセージ	RS センターシステムからデバイスのファームウェア更新要求を受けた際のメッセージを表示します。

通信テストコール

本機と RS センターシステムが接続されているかどうかをテストします。[メンテナンス] - [通信テストコール] をクリックすると、本画面が表示されます。

重要

- [通信テストコール] は、サービス実施店からの依頼があった場合だけ行います。



項目名	項目説明
テスト開始（ボタン）	本機から RS センターシステムへテストコールを行います。
ログ	通信テストコールの結果として、RS センターシステムからのステータスメッセージを表示します。

補足

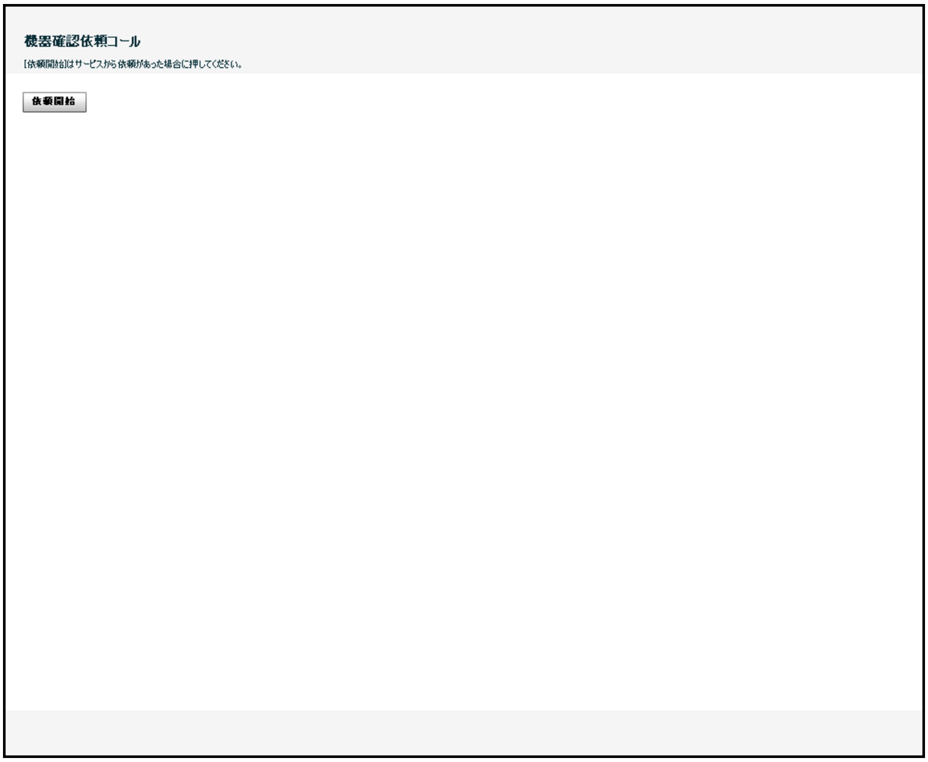
- [通信テストコール] の結果（ここでは [ログ] の内容）は RS センターシステムには送信されません。これは、本機の通信テストだけの機能です。

機器確認依頼コール

本機とRSセンターシステムが接続されているかどうかをテストし、その結果をRSセンターシステムに通知します。[メンテナンス] - [機器確認依頼コール] をクリックすると、本画面が表示されます。

重要

- [機器確認依頼コール] は、サービス実施店からの依頼があった場合だけ行います。
- [機器確認依頼コール] を使ってテストコールを行うと、本機の状態が、RSセンターシステムに通知されます。



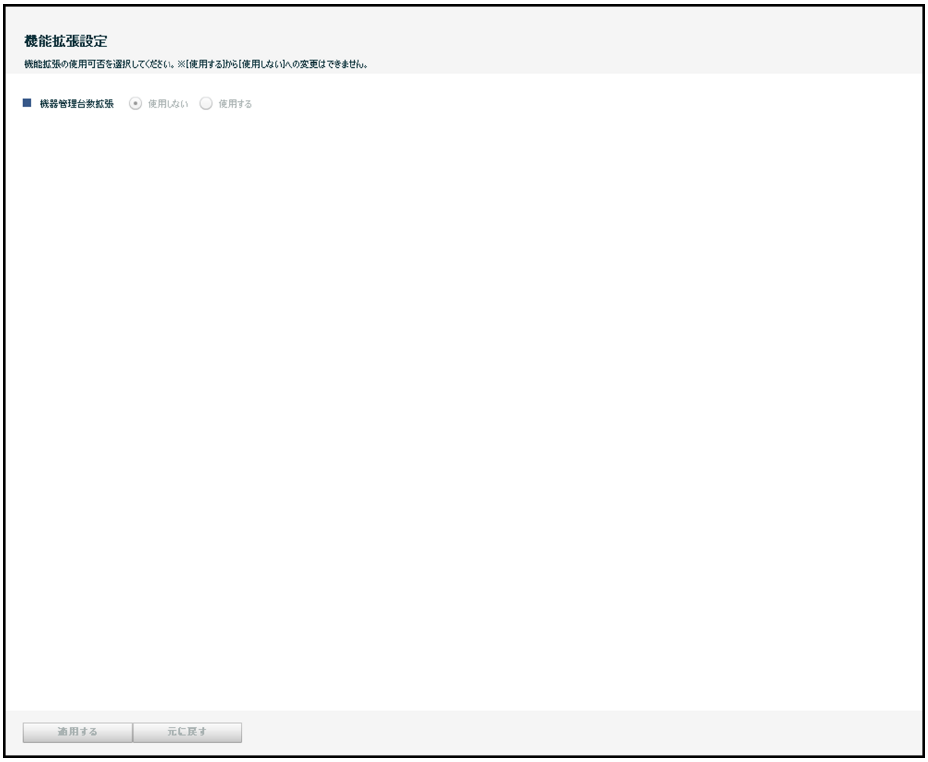
項目名	項目説明
依頼開始（ボタン）	本機からRSセンターシステムへテストコールを行います。

機能拡張設定

デバイスの登録可能台数を、100台から1,000台に拡張できます。[メンテナンス] - [機器管理台数拡張] をクリックすると、本画面が表示されます。

4

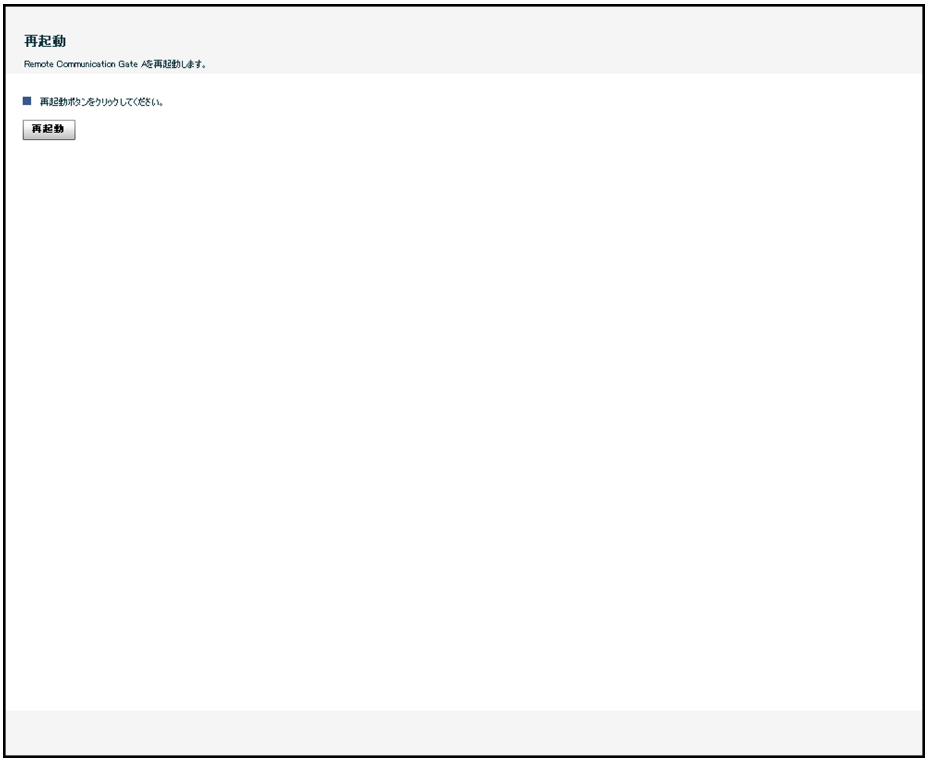
本機能は、オプションでメモリーおよびストレージが拡張されている場合に有効になります。ただし、管理者でログインした場合でも設定の変更はできません。設定を変更したい場合は、サービス実施店にご連絡ください。



項目名	項目説明
機器管理台数拡張	デバイスの管理台数を拡張するかしないかを設定します。拡張する場合は、［使用する］を選択し本機を再起動します。 いったん［使用する］に設定すると、［使用しない］に変更できません。［使用しない］に戻したい場合は、サービス実施店にご連絡ください。

RC Gate 再起動

本機を強制的に再起動できます。［メンテナンス］-［RC Gate 再起動］をクリックすると、本画面が表示されます。



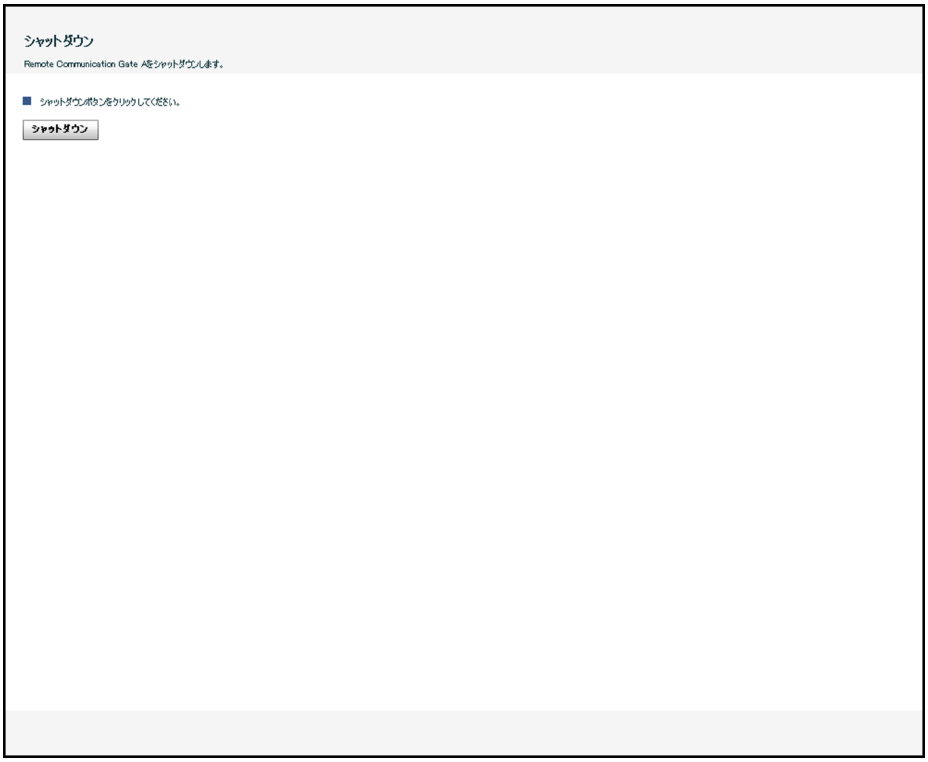
項目名	項目説明
再起動（ボタン）	本機を再起動します。再起動には数分かかります。本機の緑色の LED が点灯していることを確認してから、各操作を行ってください。

RC Gate シャットダウン

本機をシャットダウンする方法を説明します。［メンテナンス］-［RC Gate シャットダウン］をクリックすると、本画面が表示されます。

重要

- **電源プラグを抜く前にシャットダウンが完了していないと、記憶媒体が破損する場合があります。その際、最新ログが最大で 1 時間分失われることがあります。電源プラグを抜く前には、必ずシャットダウンしてください。**



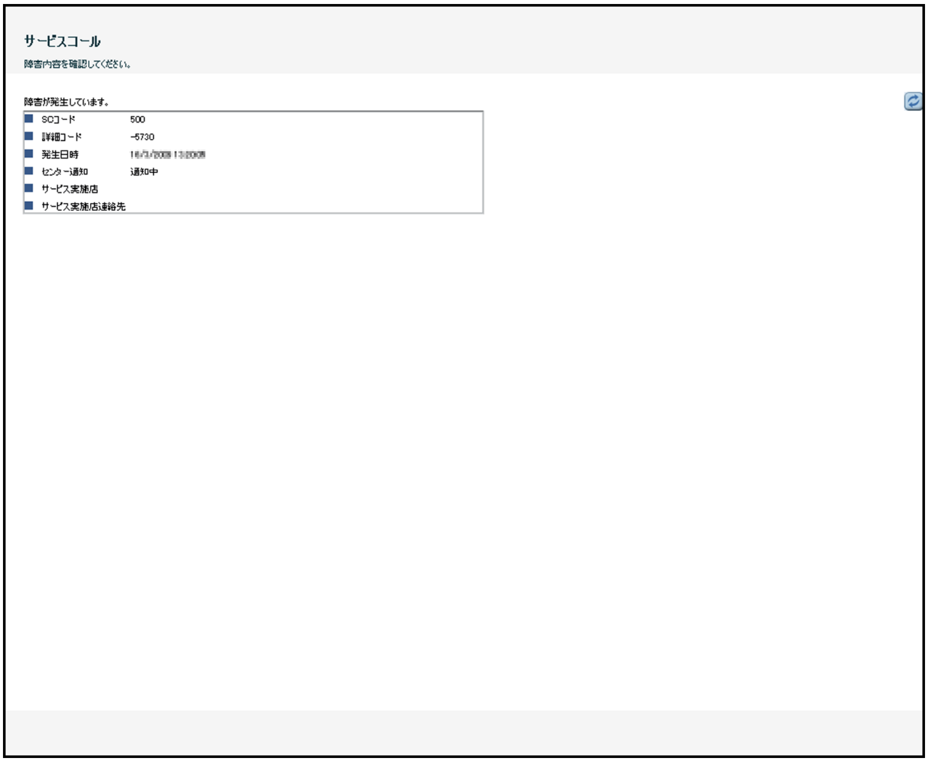
項目名	項目説明
シャットダウン（ボタン）	本機をシャットダウンします。
シャットダウン（ダイアログ）	［シャットダウン］をクリックすると、表示されます。 ［OK］をクリックすると、シャットダウン処理が開始され、「RC Gate シャットダウン中」画面が表示されます。本機のオレンジ色の LED が点滅から点灯に変わり、また緑色の LED が点灯していることを確認してから、電源を切ってください。

補足

- 本機前面にある Shutdown ボタンでもシャットダウンできます。Shutdown ボタンを 5 秒以上押し続けると、本機がシャットダウンします。

サービスコール（障害情報）

本機に障害が発生した場合、エラーコード等の情報を表示する画面です。［RC Gate 情報確認/設定］のメニュー操作中に障害が発生すると自動的に表示されるほか、［メンテナンス］-［サービスコール］をクリックすると表示されます。ウィザード中に障害発生のメッセージが表示された場合は、［戻る］をクリックすると本画面が表示されます。



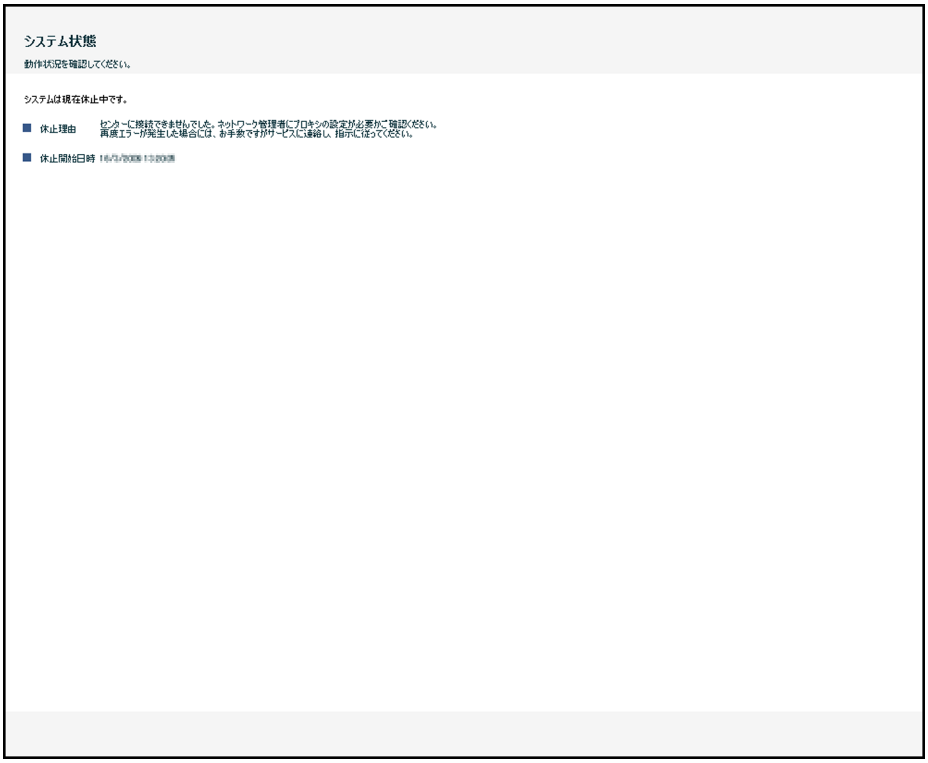
項目名	項目説明
（本機の状態）	本機に障害が発生しているかどうかを表示します。正常に動作している場合は、以下の項目は表示されません。
SC コード	本機の障害に関するエラーコードです。
詳細コード	サービスコールの種類をコードで表示します。
発生日時	障害が発生した日時です。
センター通知	RS センターシステムに対する通知の状態です。 • 通知不要 • 通知中 • 通知済み • 通知失敗
サービス実施店	本機の取扱店です。
サービス実施店連絡先	本機の取扱店の電話番号です。

補足

- 障害が発生したときは、P.141「こんなときには」を参照してください。

システム状態

本機のシステムの状態を表示する画面です。[メンテナンス] - [システム状態] をクリックすると、本画面が表示されます。また、本機が休止状態になった場合、管理者宛てに「センター接続休止通知」メールが送信されます。メール内の URL リンクをクリックすると、RC Gate モニターが起動し、ログイン後すぐに本画面が表示されます。



項目名	項目説明
(本機の状態)	本機が正常に動作しているかシステム休止かのどちらかを表示します。正常に動作している場合、以下の項目は表示されません。
休止理由	休止の主な原因と対策です。
休止開始日時	休止状態になった時刻です。

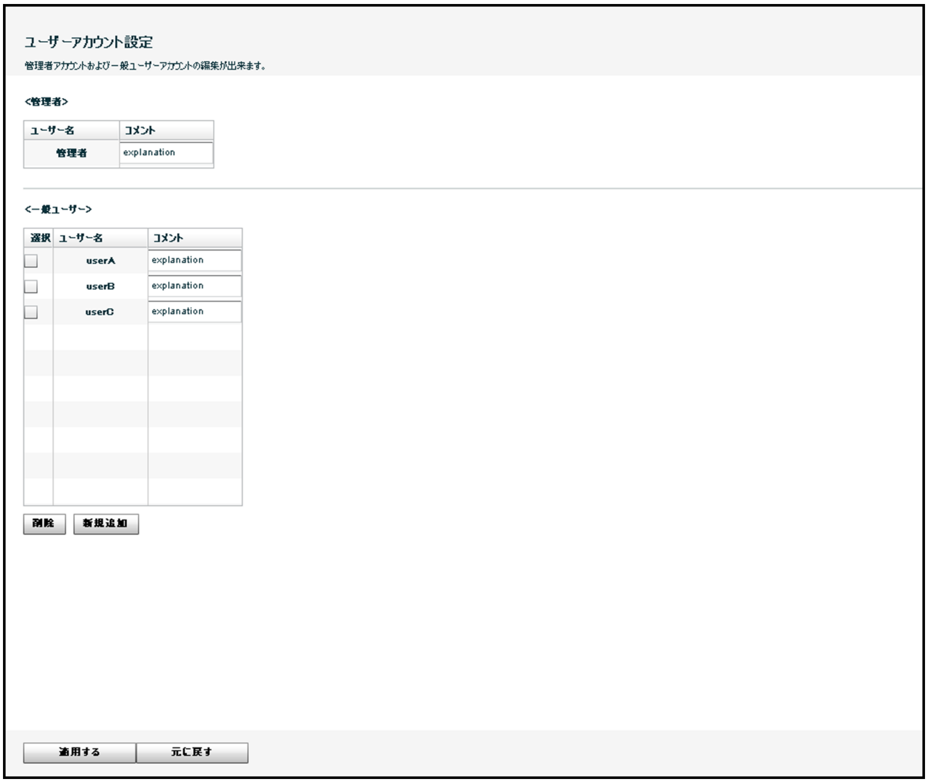
補足

- システム休止の場合は、以下の項目をチェックしてください。
    - パスワードをはじめ、プロキシに関する設定が変更になっていないこと。
    - 本機につながっているネットワークケーブルが抜けていないこと。
    - 本機につながっているハブなどのネットワーク機器の電源が入っていること。

- 以上の項目を解決してもシステムが休止した状態の場合は、サービス実施店にご連絡ください。

ユーザーアカウント設定

RC Gate モニターにログインするアカウントの一覧を閲覧できます。[セキュリティ] - [ユーザーアカウント設定] をクリックすると、本画面が表示されます。



<管理者>

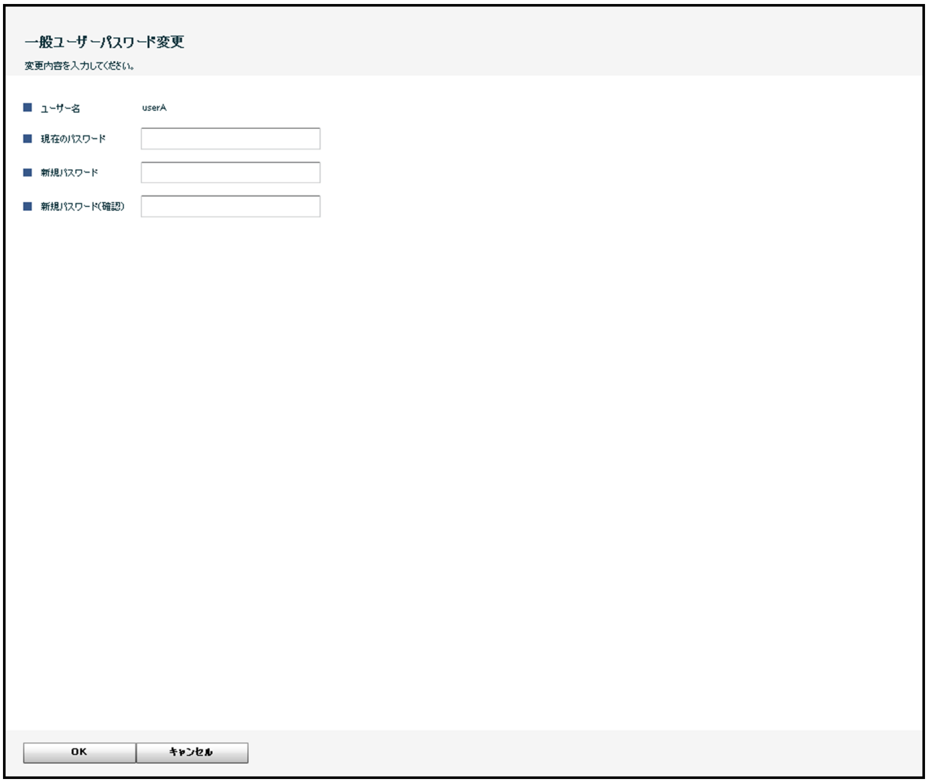
項目名	項目説明
ユーザー名	管理者アカウントのログインユーザー名です。管理者のパスワードを変更したい場合は、ユーザー名をクリックします。
コメント	ユーザーの説明です。

<一般ユーザー>

項目名	項目説明
ユーザー名	一般ユーザーアカウントのログインユーザー名です。一般ユーザーのパスワードを変更したい場合は、ユーザー名をクリックします。
コメント	ユーザーの説明です。
削除（ボタン）	選択した一般ユーザーアカウントのログインユーザー名が削除されます。
新規追加（ボタン）	「一般ユーザー新規追加」画面が表示されます。最大で 10 ユーザー登録できます。

パスワード

RC Gate モニターログイン時のパスワードを変更できます。[セキュリティ] - [ユーザーアカウント設定] - [パスワード] をクリックし、パスワードを変更したいユーザー名をクリックすると、本画面が表示されます。



重要

- ユーザー名は 1 ～ 13 文字（ASCII 文字）で設定してください。

- ユーザー名として使用できるのは、以下の英数と（スペース）、「-」、「_」の ASCII 文字だけです。((スペース) - 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _ a b c d e f g h i j k l m n o p q r s t u v w x y z)
- 上記以外の文字はユーザー名としては使えません。
- パスワードは工場出荷時のままではご使用にならず、変更してお使いください。新しいパスワードは 8～13 文字（ASCII 文字）で設定してください。
- パスワードとして使用できるのは、以下の ASCII 文字だけです。((スペース) ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [¥] ^ _ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ‾)
- 「以下の項目が不適切です。[OK]を押して元の画面に戻り、正しく設定してください。」というエラーメッセージが表示されたときは、ユーザー名またはパスワードについて、使用可能な文字であるか、また使用文字数の範囲内であるかどうかを確認し再設定してください。
- 管理者は、自身と一般ユーザーのパスワードを半年以内の周期で変更してください。
- 辞書にあるような単語や同じ文字の繰り返しなど、容易に類推される単語はパスワードとして利用しないでください。
- パスワードを書き留めて、机など人目にふれるところに貼らないでください。

補足

- 新パスワードは、次回のログインから有効になります。

項目名	項目説明
ユーザー名	ログインユーザー名です。
現在のパスワード	現在設定されているパスワードを入力します。
新規パスワード	新しいパスワードを入力します。
新規パスワード（確認）	入力ミス等を防ぐために、新しいパスワードを再度入力します。

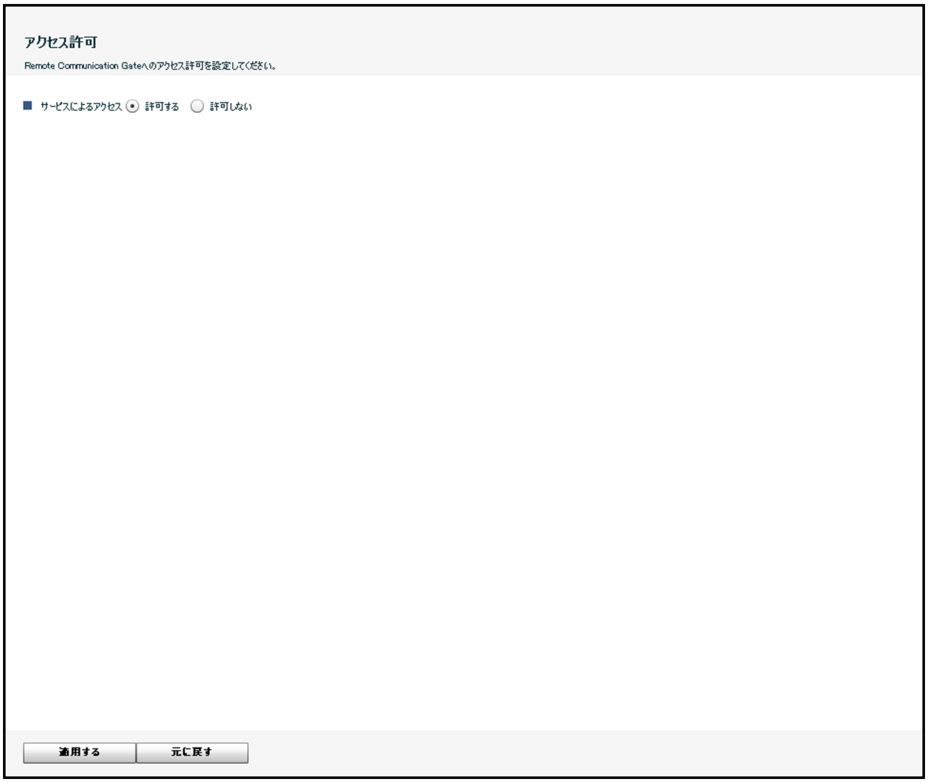
アクセス許可

カスタマーエンジニアのアクセス許可および、RS センターシステムからの RC Gate ファームウェア更新許可を設定します。［セキュリティ］-［アクセス許可］をクリックすると、本画面が表示されます。

重要

- 「サービスによるアクセス」では、カスタマーエンジニアが点検や修理をする際、本機にアクセスできるかどうかを設定します。ここで［許可しない］に設定すると、管理者が「サービスによるアクセス」を［許可する］に設定するまで、カスタマーエンジニアが本機にアクセスして点検や修理を行うことができなくなります。そのため、適切なサービスが受けられない場合があります。一方、常に［許可する］に設定した

運用では、カスタマーエンジニアになりすました攻撃を受けるリスクがあります。通常は［許可しない］と設定しておき、点検や修理が必要な時だけ［許可する］に変更するのが、より安全な運用です。なお、メンテナンスは専任のカスタマーエンジニアをご指名ください。



項目名	項目説明
サービスによるアクセス	カスタマーエンジニアによる本機へのアクセスを、許可するかどうか選択します。 カスタマーエンジニアによるアクセスを許可する場合は、［許可する］を選択してください。

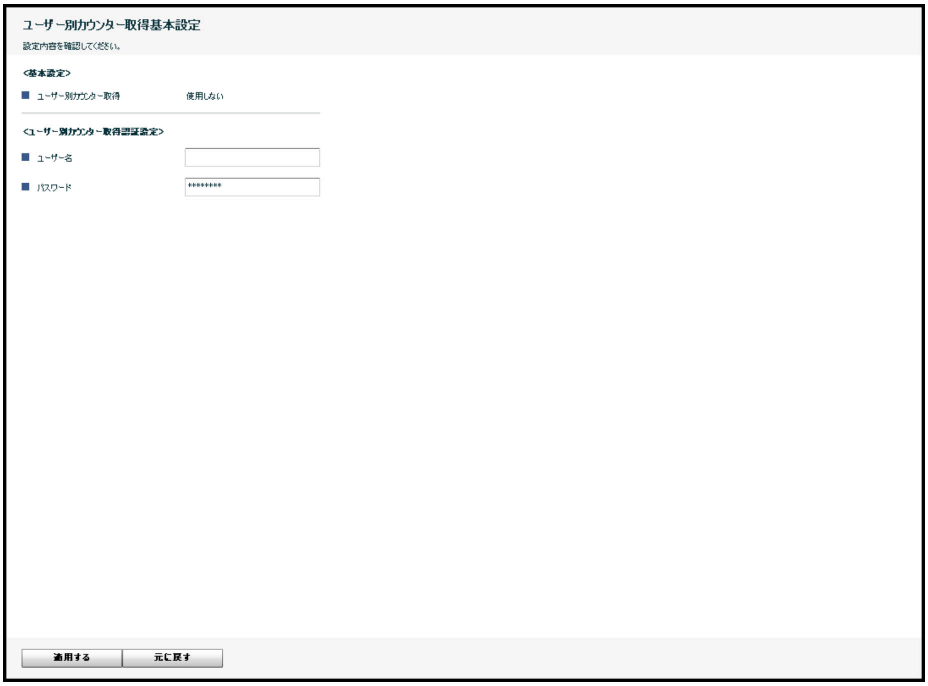
ユーザー別カウンター取得基本設定

RS センターシステムから指定されたデバイスのカウンター情報を、ユーザー別に収集して処理できます。［ユーザー別カウンター］-［ユーザー別カウンター取得基本設定］をクリックすると、本画面が表示されます。

本機能は、以下の 2 つの条件が満たされたときに有効になります。

- オプションでメモリーが拡張されている場合
- アプリケーションバージョンが 2.05 以上の場合

なお、ユーザー別カウンター取得時のデバイスと RC Gate 間の通信データは暗号化されません。



項目名	項目説明
ユーザー別カウンター取得	ユーザー別カウンターの取得機能が動作するかどうかを表示します。
ユーザー名	ユーザー別カウンター取得のためにデバイスにアクセスするとき、認証に使用する機器管理者のユーザー名を入力します。
パスワード	ユーザー別カウンター取得のためにデバイスにアクセスするとき、認証に使用する機器管理者のパスワードを入力します。

ユーザー別カウンターを取得するためには、対象機器のデバイス管理者のユーザー名とパスワードの入力が必要です。セキュリティ認証（CC）を取得した製品として本機をご使用のお客様は、デバイス管理者のユーザー名とパスワードは入力しないで下さい。

ユーザー別カウンター取得対象機器一覧

ユーザー別カウンターを取得する場合に、情報取得対象のデバイスを一覧表示します。

［ユーザー別カウンター］-［ユーザー別カウンター取得対象機器一覧］をクリックすると、本画面が表示されます。



項目名	項目説明
ユーザー名	ユーザー別カウンター取得のために、デバイスにアクセスする際に認証に使用する機器管理者のユーザー名を入力します。
パスワード	ユーザー別カウンター取得のために、デバイスにアクセスする際に認証に使用する機器管理者のパスワードを入力します。
選択行へコピー	[選択行へコピー] をクリックすると、機器一覧中の選択されたデバイス情報に対して、入力されたユーザー名、パスワードでの更新を行います。
すべての表示中項目を選択	[すべての表示中項目を選択] をクリックすると、機器一覧で表示されているすべてのデバイスが選択状態になります。
すべての表示中項目を選択解除	[すべての表示中項目を選択解除] をクリックすると、機器一覧で表示されているすべてのデバイスが非選択状態になります。
認証テスト	[認証テスト] をクリックすると、機器一覧で選択されているデバイスに対して、ユーザー別カウンター情報が取得できるかどうか確認を行い、その確認結果を表示します。

ユーザー別カウンター取得テスト

ユーザー別カウンターを取得できるかどうかを確認します。[ユーザー別カウンター] - [ユーザー別カウンター取得テスト] をクリックすると、本画面が表示されます。



項目名	項目説明
IP アドレス	ユーザー別カウンターの取得可否をテストするデバイスの IP アドレスを入力します。
ユーザー名	ユーザー別カウンター取得のために、デバイスにアクセスする際に認証に使用する機器管理者のユーザー名を入力します。
パスワード	ユーザー別カウンター取得のために、デバイスにアクセスする際に認証に使用する機器管理者のパスワードを入力します。
取得テスト	[取得テスト] をクリックして、テスト結果を表示します。
結果	ユーザー別カウンターの情報取得が成功したかどうかを表示します。
機番	ユーザー別カウンターの情報取得を行ったデバイスの ID を表示します。
カウンター詳細	取得したユーザー別カウンター情報を表示します。

4

@Remote サービス機能制限

@Remote サービス機能を停止できます。[セキュリティ] - [@Remote サービス機能制限] をクリックすると、本画面が表示されます。

重要

- 「センターによるシステムファームウェア更新」では、本機ファームウェア（アプリケーション、ファームウェア共通部、プラットフォーム、OS）の最新のバージョンを RS センターシステムから受信する際、[許可する] を選択してください。工場出荷時のバージョンを継続して使用する場合は、[許可しない] を選択してください。



<@Remote サービス機能>

項目名	項目説明
@Remote サービス機能	[制限する] を選択すると、RS センターシステムとデバイスの通信が制限されます。

<センターからの要求可否設定>

項目名	項目説明
センターによるシステムファームウェア更新	センターによるシステムファームウェアの更新を、許可するかどうか選択します。
センターによる機器ファームウェア更新	センターによるデバイスのファームウェア更新方針の選択を、許可するかどうか選択します。

項目名	項目説明
センターによるオートディスカバリー設定	センターによるオートディスカバリーを、許可するかどうか選択します。

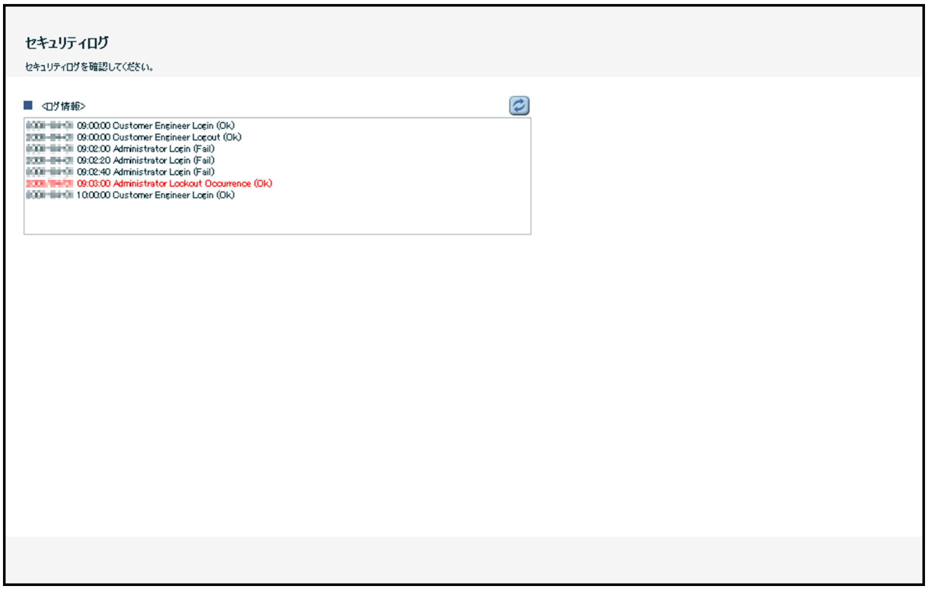
セキュリティログ

ログイン、ログアウト、システム更新等のセキュリティ関連情報を表示します。[セキュリティ] - [セキュリティログ] をクリックすると、本画面が表示されます。

[最新の情報に更新] をクリックすると、最新のログ情報を取得します。

重要

- 以下の使用環境では、1 日に約 28 件のログが記録されます。ログ領域には最小で 5,824 件の記録が可能なため、約 208 日分のログ情報を保持できます（5,824 ÷ 28 = 208）。
    - 管理者および一般ユーザーが、それぞれ 1 日 1 回ログイン／ログアウトする。
    - デバイスのポーリングが 1 時間に 1 回発生する。
- 未確認のログ情報が上書きされるのを防ぐため、最低でも 104 日（約 15 週）に 1 度はログ情報を確認することをお勧めします。
- セキュリティログの件数が最大保持件数を超えると、古いログ情報は確認の有無にかかわらず上書きされます。
- ログを確認するときは、管理者自身の直近のログイン記録が表示されていることを必ず確認してください。直近のログイン記録が確認できないときは、サービス実施店にご連絡ください。



4

セキュリティログ 1 件につき、以下の表に示す情報が表示されます。

項目名	項目説明
日付・時刻	ログ情報が記録された日付と時刻（UTC 時刻）です。以下の形式で表示されます。 y-m-d H:M:S y: 西暦、m: 月、d: 日、H: 時、M: 分、S: 秒
ユーザー	RC Gate にアクセスしたユーザーのタイプです。 • RS センターシステムの場合："Communication Server" • システムの場合："System"*1 • カスタマーエンジニアの場合："Customer Engineer" • 管理者の場合："Administrator" • 一般ユーザーの場合："User（*************）"*2
アクセス内容	ログの発生要因 • 電源 ON（起動）の場合："Logging Start" • 電源 OFF（シャットダウン、再起動）の場合："Logging End" • システムログ読み出しの場合："Get SystemLog"*3 • 通信ログ読み出しの場合："Get CommunicationLog"*3 • セキュリティログ読み出しの場合："Get SecurityLog" • ログインの場合："Login" • ログアウトの場合："Logout" • ロックアウト発生の場合："Lockout Occurrence" • カスタマーエンジニアアカウント情報変更の場合："Changes to CE Account" • 管理者アカウント情報変更の場合："Changes to ADMIN Account" • 一般ユーザーアカウント情報変更の場合：" Changes to USER（*************） Account"*2 • 一般ユーザーアカウント追加の場合："Add USER（*************） Account"*2 • 一般ユーザーアカウント削除の場合："Delete USER（*************） Account"*2 • 時刻変更の場合："Adjust Clock" • システムファームウェア更新の場合："System Firmware Update" • SSL 通信異常発生の場合："SSL Communication" • デバイス認証情報更新の場合："Device Certificate Update" • 証明書更新の場合："System Certificate Update" • 自己診断の場合："Self Check" • システムファームウェア正当確認の場合："System Firmware Check"
アクセス結果	• 成功の場合："（OK）" • 失敗の場合："（Fail）"
項目区切り	（空白）

項目名	項目説明
項目区切り	":"（コロン）
レコード区切り	"¥n"（改行）

*1 "System"は、RC Gate 本体です。

*2 "*************"は、ユーザーアカウント名の最初の 13 文字です。

*3 "System log"と"Communication log"は保守用のため、管理者は確認できません。

5. 付録

RC Gate の画面に表示されるメッセージ

以下の表は、RC Gate の画面に表示されるメッセージの説明です。

1 行目

メッセージ	説明
Warming Up	システムの起動処理を実施中です。
Not Set Up	@Remote サービス登録が完了していません。
Normal	@Remote サービス登録が完了し、通常動作している状態です。
Off-line	RS センターシステムとの通信が中断されています。
Error	システム異常が発生しています。
Call Service Rep	異常状態になり、再起動を規定の回数行っても復旧しない状態です。
Not in Service	@Remote サービス機能制限により、@Remote サービスが制限されている状態です。
Reboot	システムの再起動を実施中です。
Shutdown	システムの終了処理を実施中です。

2 行目

メッセージ	説明
SC:	システムに異常が発生しているか、システムが異常停止しています。最大で 6 桁の異常ステータスコードを表示します。サービス実施店にご相談ください。
Cable Disconnect	ケーブルが正しく接続されていないか断線しています。ケーブルの接続を確認してください。
802 Server Error	IEEE802.1x 認証をご利用の場合に、IEEE802.1x 認証サーバーへの接続が出来ない状態です。ネットワーク管理者にご相談ください。
802 Auth.Failure	IEEE802.1x 認証をご利用の場合に、IEEE802.1x 認証に失敗しています。ネットワーク管理者にご相談ください。
DHCPv6 Error	DHCPv6 設定が有効のときに、IP アドレスの取得に失敗しています。ネットワーク管理者にご相談ください。
DHCPv4 Error	DHCPv4 設定が有効のときに、IP アドレスの取得に失敗しています。ネットワーク管理者にご相談ください。
---------------	起動処理中、または終了処理中に表示されます。

メッセージ	説明
ネットワーク情報・ホスト名 “ホスト名” ネットワーク情報・IPv6 設定 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx ネットワーク情報・IPv4 設定 xxx.xxx.xxx.xxx（x は IP アドレスの数値）	本機のホスト名、LAN ポートで使用している本機 IPv6 アドレス、LAN ポートで使用している本機 IPv4 アドレスが順に表示されます。

5

こんなときには

エラーメッセージが表示された

メッセージ	発生事由と対処方法
選択を必要とする項目が選択されていません。[戻る] を押して元の画面に戻り、項目を選択してください。	「機器登録ウィザード：検索結果」画面で、「選択」欄にチェックが 1 つも入っていません。[戻る] で「機器登録ウィザード：検索結果」画面に戻り、登録するデバイスの「選択」欄にチェックを入れてください。
内部エラー システムエラーが発生しました。お手数ですがサービスに連絡し、指示に従ってください。 -（4 桁のエラーコード）	システム内部でエラーが発生しています。エラーコードを、サービス実施店にご連絡ください。
回線がビジーのため制限時間内に処理が正常に終了しませんでした。しばらくたってからもう一度実行してください。再度エラーが発生した場合には、お手数ですがサービスに連絡し、指示に従ってください。	RS センターシステムの DB 障害やプログラム障害が発生しています。しばらく時間を置いても復旧しない場合は、サービス実施店にご連絡ください。
お申込み受け付け番号を確認し、もう一度実行してください。再度エラーが発生した場合には、お手数ですがサービスに連絡し、指示に従ってください。	正しいお申込み受け付け番号を入力しているにもかかわらず、エラーが発生した場合は、以下のような RS センターシステム登録情報との不整合が原因です。 • 該当デバイスが RS センターシステムに登録されていない／されている • 依頼区分が異なる サービス実施店にご連絡ください。
不正なアクセスです。ログインし直してください。	Web ブラウザーのウィンドウを複数開き、そのうちの一つのウィンドウで設定を行い、別のウィンドウで確定処理を行った場合に、このエラーが発生します（無効なアクセスの場合を除きます）。設定時には、Web ブラウザーでウィンドウを複数開かないでください。
この機能を実行する権限がありません。 Remote Communication Gate 管理者に設定を確認してください。	5 分間で 3 回ログインに失敗すると、本機へのログインが禁止になります。1 分後に再度ログインが可能です。

エラーメッセージに示された障害が継続する場合

エラーメッセージに示された障害が継続する場合は、サービス実施店にお問い合わせください。

事業所の移転、デバイスの移動等

以下の場合は、事前に RS センターシステム側 DB への登録手続きが必要です。サービス実施店までお問い合わせください。

- 事業所の移転（本機の移動）
- デバイスの移動（オートディスカバリーを除く）
- デバイスの新設（オートディスカバリーを除く）
- デバイスの削除（オートディスカバリーを除く）

本機を返却する場合

運用を終了するときは、お客様の情報を守るために本機を回収し、本機に登録された情報を削除します。サービス実施店にご連絡ください。

エラーコード

エラーコード	メッセージ
0001	ネットワーク接続に失敗しました。LAN ケーブルが接続されているか確認してください。
0002	ネットワーク接続に失敗しました。 DHCP を利用している場合は、ネットワーク設定を確認してください。 再度エラーが発生した場合には、お手数ですがサービスに連絡し、指示に従ってください。
0003	IEEE802.1x 認証に失敗しました。ネットワーク管理者に確認してください。 再度エラーが発生した場合には、お手数ですが、サービスに連絡し、指示に従ってください。
0004	IEEE802.1x 認証に失敗しました。IEEE802.1x 認証の設定を確認してください。 再度エラーが発生した場合には、お手数ですがサービスに連絡し、指示に従ってください。
0005	ネットワーク接続に失敗しました。ネットワーク設定の DNS を確認してください。 再度エラーが発生した場合には、お手数ですがサービスに連絡し、指示に従ってください。
0006	ネットワーク接続に失敗しました。プロキシサーバー名、ポート番号を確認してください。

エラーコード	メッセージ
0007	ネットワーク接続に失敗しました。プロキシユーザー名、プロキシパスワード、または、プロキシドメイン名を確認してください。
1001	センターに接続できませんでした。 お手数ですがサービスに連絡し、指示に従ってください。
1002	センターに接続できませんでした。 お手数ですがサービスに連絡し、指示に従ってください。
1003	センターに接続できませんでした。 お手数ですがサービスに連絡し、指示に従ってください。
1004	センターとの通信に失敗しました。 お手数ですがサービスに連絡し、指示に従ってください。
1005	センターとの通信に失敗しました。 お手数ですがサービスに連絡し、指示に従ってください。

初期値一覧

項目	初期値	補足
表示言語(Language)	日本語	
タイムゾーン	(GMT +09:00)Osaka,Sapporo,Tokyo	
IP アドレス送信許可設定	許可する（デフォルト）	
DHCP	無効	
サブネットマスク	255.255.255.0	各ネットワーク設定画面
イーサネット速度	自動選択	
プロキシサーバー	無効	
プロキシポート番号	8080	
RC Gate メールアドレス（送信者用）	rc_gate	
メール再送信回数	3 回	
メール再送信間隔時間	15 秒	
SMTP サーバーポート番号	25	
SMTP_AUTH	無効	
POP before SMTP	無効	
POP サーバーポート番号	110	
サービスによるアクセス	許可する	

項目	初期値	補足
センターによるシステムファームウェア更新	許可する	
センターによる機器ファームウェア更新	許可する	
センターによるオートディスカバリー設定	許可する	
IP アドレス検索範囲	0.0.0.0-0.0.0.0	「オートディスカバリー設定ウィザード」、「機器登録ウィザード」利用時
SNMP コミュニティ名	public	「オートディスカバリー設定ウィザード」、「機器登録ウィザード」利用時
表示件数	10 件	「オートディスカバリー設定ウィザード」、「機器登録ウィザード」利用時

本体仕様

項目	内容	
形式	ボックスタイプ	
インターフェース	Ethernet インターフェース×2 （10BASE-T または 100BASE-TX）	
オプション	• Remote Communication Gate Memory 1000 • Remote Communication Gate Storage 1000	
表示部	LED	2 個（Alert、Power）
	画面	LCD（16 桁×2 行）
主なサービス機能	カウンター自動検針 遠隔診断保守（リモート点検/SC、CC、AC、MC 通報とコール時対応） 使用枚数等情報提供（ご使用状況報告） トナーエンド情報提供 ファームウェアのリモート更新	
対応プロトコル	TCP/IP、SNMP、HTTP、SOAP、SMTP、DHCP	
管理対象デバイス	当サービス対応のデジタル複合機、コピー機、プリンター	
最大接続台数	• RS センターシステムに登録した管理対象デバイス 100 台（オプションでメモリー・ストレージ拡張時は 1,000 台） • オートディスカバリー 1,000 台（RS センターシステムに登録したネットワーク上のデバイスも含む）	
使用環境	10～32℃、15～80%RH	
電源	AC100V±10%、50/60Hz±3Hz	
消費電力	20W 以下	
大きさ	幅 253mm/奥行き 160mm/高さ 48mm	
重量	800g	

電波障害に関する注意事項

ほかのエレクトロニクス機器に隣接して設置した場合、お互いに悪影響を及ぼすことがあります。特に、近くにテレビやラジオなどがある場合、雑音が入ることがあります。その場合は、次のようにしてください。

- テレビやラジオなどからできるだけ離す。
- テレビやラジオなどのアンテナの向きを変える。

- コンセントを別にする。

補足

- この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。使用説明書に従って正しい取り扱いをしてください。

リサイクル部品について

リコーは環境保全を経営の優先課題のひとつと考え、リサイクル推進にも注力しております。

本製品には、新品と同一の当社品質基準に適合した、リサイクル部品を使用している場合があります。

本機に搭載されているソフトウェアの著作権などに関する情報

本機に搭載されているソフトウェアは、以下を含みます。

- WPASupplicant
- OpenSSL
- busybox
- dosfstools
- glibc
- knopflerfish
- corelib
- as3crypto
- as3httpclientlib
- SNMP4J
- kxml2
- Apache commons
- kSOAP2
- linux-kernel
- Dibbler
- BouncyCastle
- AspectJ

これらのソフトウェアのライセンス・著作権等に関する情報は、RC Gate モニターのログイン画面から［ライセンス・著作権情報］のリンクをクリックするとご覧になれます。

索引

記号・数字

アルファベット

あ

か

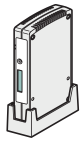
さ

MEMO

MEMO

株式会社 リコー
東京都中央区銀座8-13-1 リコービル 〒104-8222
http://www.ricoh.co.jp/

Remote Communication Gate A 使用説明書



お問い合わせ先

製品についてのお問い合わせはサービス実施店にご連絡ください。
転居の際は、サービス実施店または販売店にご連絡ください。転居先の最寄りのサービス実施店、販売店をご紹介いたします。

JA (JP) 2013年4月 D459-8501B